Haaga-Helia
ammattikorkeakoulu Oy

Tietoturvan päivittäminen vastaamaan EU:n tietosuoja-asetusta

Rauno Saarnio

Opinnäytetyö
Tietojenkäsittelyn koulutusohjelma
2017

Haaga-Helia ammattikorkeakoulu Oy

Tiivistelmä

14.12.2017

Tekijä(t)
Rauno Saarnio

Koulutusohjelma
Tietojenkäsittelyn koulutusohjelma

Opinnäytetyön otsikko
Tietoturvan päivittäminen vastaamaan EU:n tietosuoja-asetusta

Sivu- ja liitesivumäärä
41 + 12

Opinnäytetyön otsikko englanniksi
Updating information security to the GDPR (General Data Protection Regulation)

EU:n tietosuoja-asetus astuu voimaan 25.5.2018. Asetuksen mukaan henkilörekisterin pitäjän on pystyttävä osoittamaan, että henkilötietoja käsitellään asetuksen mukaisesti. Organisaatiolla (seurakunnalla) on osoitusvelvollisuus. Osoitusvelvollisuutta tehostetaan 20 m€:n uhkasakolla. Julkishallinnon uhkasakon määrää voi vielä muuttua kansallisen lainsäädännön astuessa voimaan.

Opinnäytetyön tavoitteena oli luoda tiekartta EU:n tietosuoja-asetuksen vaatimien tehtävien tekemiseksi, sekä toteuttaa osa tehtävistä Pornaisten seurakunnassa. Tehtävä rajattiin koskemaan hallinnollista tietosuojaa, eli työstä rajattiin pois käytännön tietoturvan toimenpiteet. Myös kirkon yhteisten tietojärjestelmien käsittely rajattiin työn ulkopuolelle.

Työ aloitettiin laatimalla karkean tason projektisuunnitelma. Projektisuunnitelman päävaiheet ovat: Johdon tahtotilan määrittely, ohjeistus ja koulutus, analyysit ja kehittäminen, seuranta ja raportointi.

Kirjoitimme aluksi seurakunnan tietosuoja- ja tietoturvapolitiikat ja selosteen käsittelytoimista. Laadimme aluksi myös Excel-pohjaisen päiväkirjan osoitusvelvollisuutta täyttääksemme. Kävimme edellä mainitut dokumentit läpi työntekijäkokouksessa, jossa velvoitimme henkilöstön katsomaan arjentietosuoja.fi sivuilla olevan tietoiskun ja tekemään tietosuojatestin. Testin tulos on toimitettava talouspäällikölle vuoden 2017 loppuun mennessä.

Kirkkoneuvosto ja kirkkovaltuusto ovat kokouksissaan käsitelleet tietosuoja-asetusta.

Hanke eteni kartoittamalla ja analysoimalla keskeiset sopimukset ja rekisterit. Analyysin perusteella päädyimme keskittämään luottamushenkilöiden ja vapaaehtoisten henkilörekisterit yhteen rekisteriin. Totesimme, ettemme muuten voi täyttää EU:n tietosuoja-asetuksen vaatimuksia. Keskitetyn rekisterin valinta on vielä kesken. Olemme tehneet työtä SCRUM-metodin mukaisin nopein sprintein, käytännössä työn alla on koko ajan ollut projektisuunnitelman kustakin päävaiheesta jokin tehtävä. Toteutustyö on kesken, mutta malli on osoittanut toimivuutensa Pornaisten seurakunnassa.

Asiasanat
tietosuoja-asetus, GDPR, henkilörekisteri, henkilötieto, seurakunta, arkaluontoinen henkilötieto

Sisällys

1 Johdanto

Toimin pienen seurakunnan talouspäällikkönä, jonka yksi tehtäväalue on vastata tietoturvasta ja -suojasta. EU:n tietosuoja-asetus astuu voimaan 25.5.2018, tämä aiheuttaa toimenpiteitä seurakunnissa. Tavoitteena on, että kyse ei ole kertaluonteisesta projektista vaan prosessista, joka jää elämään työyhteisössä. Tietosuoja-asetuksen vaatimat toimenpiteet tulee tehdä, koska tietoturvaloukkauksista on määritelty maksimissaan 20 m€:n uhkasakko. Tietosuojan pettäminen on seurakunnan maineen kannalta äärimmäisen ikävä asia, seurakunnan toimintaan pitää voida luottaa kaikessa.

Opinnäyte työn toimeksiantajana on Pornaisten seurakunta (evl).

Haluan selvittää opinnäytetyössä:

- Mihin toimintoihin EU:n tietosuoja-asetus vaikuttaa?
- Miten se vaikuttaa käytäntöihin?
- Miten se otetaan käyttöön ja ylläpidetään?

Lukijalta odotetaan perusymmärrystä tietoturvasta ja tietosuojasta. Työssä ei käsitellä fyysistä tietoturvaa eikä seurakunnan käyttämien valtakunnallisten tietojärjestelmien tietoturvaa. Seurakunnan tietoteknisistä ratkaisuista, ohjelmistojen ja tietoliikenteen turvallisuudesta vastaavat pääsääntöisesti kirkon eri palvelukeskukset tai keskushallinto. Tässä työssä käsitellään erityisesti tiedon käsittelyyn liittyvää tietoturvaa.

Opinnäytetyön tuotoksena syntyy työohje tietosuoja-asetuksen käyttöönottamiseksi. Työohje kirjoitetaan henkilölle joka ei ole it-ammattilainen. Tavoitteena on, että kuka tahansa ei it-alan ammattilainen pystyy tämän pohjalta toteuttamaan EU:n tietosuoja-asetuksen mukaiset vaatimukset seurakunnassa ja muissa vastaavan kaltaisissa yhteisöissä.

Työn keskeiset käsitteet ovat: tietosuoja-asetus, GDPR, henkilörekisteri, henkilötieto, arkaluonteinen henkilötieto, seurakunta.

EU:n tietosuoja-asetus määrittelee miten luonnollisten henkilöiden henkilötietoja saa käsitellä sekä miten henkilötietoja tulee suojella. GDPR (General Data Protection Regulation) on edellä mainittu tietosuoja-asetus. Henkilörekisteri on henkilötietoja sisältävä tietojoukko. Henkilötieto on tietoa, jonka avulla yksittäinen henkilö voidaan tunnistaa. Arkaluonteisia henkilötietoja ovat uskonnolliseen vakaumukseen, terveyteen ja jne. liittyvä henkilötieto. Seurakunta on evankelisluterilaisen kirkon itsenäinen paikallinen organisaatio.

2 Hallinnollinen tietoturva

2.1 Tietoturvan historiaa

Tietosuojan historia yltää yli 2.500 vuoden takaiseen aikaan, jolloin lääkärit ottivat käyttöön Hippokrateen valan (Suomentanut Heikki Solin), jossa vannotaan mm. ” Mikäli parannustyössäni tai sen ulkopuolella ihmisten keskuudessa näen tai kuulen sellaista, mitä ei pidä levitettämän, vaikenen ja pidän sitä salaisuutena”. Siinä on hyvä ohje myös tietotyötä tekeville ihmisille tänä päivänä. (Lääkäriliitto)

Seuraava merkittävä aikakausi olivat suuret vallankumoukset 1700-luvulla (Ranska, Hollanti, USA:n sisällissota), maailmansodat ja IT-teknologian kehittyminen 1960-luvulta lähtien. (OpiTietosuojaa.fi)

Laki tietosuojalautakunnasta ja tietosuojavaltuutetusta annettiin 20.4.1987, § 1: ” Henkilörekisterilaissa (471/87) tarkoitettujen asioiden käsittelemistä varten on oikeusministeriön yhteydessä tietosuojalautakunta ja tietosuojavaltuutetun sopimuspalkkainen virka.” Tietosuojalautakunta ratkaisee ne asiat, jotka sille on annettu päätettäväksi henkilörekisterilain mukaan (§ 3). Tietosuojavaltuutetun tehtävänä on (§ 7) seurata, ohjata ja valvoa henkilörekistereihin kerättävän ja talletettavan tiedon käyttöä, suojaamista ja luovuttamista (Laki tietosuojalautakunnasta ja tietosuojavaltuutetusta 474/1987).

2.2 Yleistä

Johdon sitoutuminen tietoturvallisuuden kehittämiseen ja perusvaatimusten ymmärtäminen luovat perustan hallinnolliselle tietoturvalle. Johdon tulee tietää ja tuntea sekä toiminta että tietojärjestelmät ja näihin liittyvät riskit. Riskien havaitsemiseksi ja toimivien käytänteiden luomiseksi tulee muodostaa tietoturvaryhmä, johon kutsutaan jäseniä organisaation eri puolilta, eli henkilöitä joilla on tietoa tiedosta ja tiedon käytöstä (Valtiovarainministeriö 2004).

Tietoturvastrategia ja / tai tietoturvapolitiikka tuovat ilmi organisaation asettamat tavoitteet ja tahtotilan. Tietoturvastrategia ja -politiikka ovat osa organisaation toiminta- ja johtamisjärjestelmää. Näiden ylätason dokumenttien tulee ohjata päivittäistä toimintaa. Johdon oma toiminta luo pohjan organisaation turvallisuuskulttuurille. Tietoturvatavoitteista on viestittävä selkeästi koko organisaatiolle (Valtiovarainministeriö 2004).

Alla olevassa kuvassa havainnollistetaan tietoturvan hallintaa, ja eri dokumenttien tarkoituksia. Organisaatiossa voi olla yksi dokumentti, jolla kuvataan tahtotila ja keinot (miten

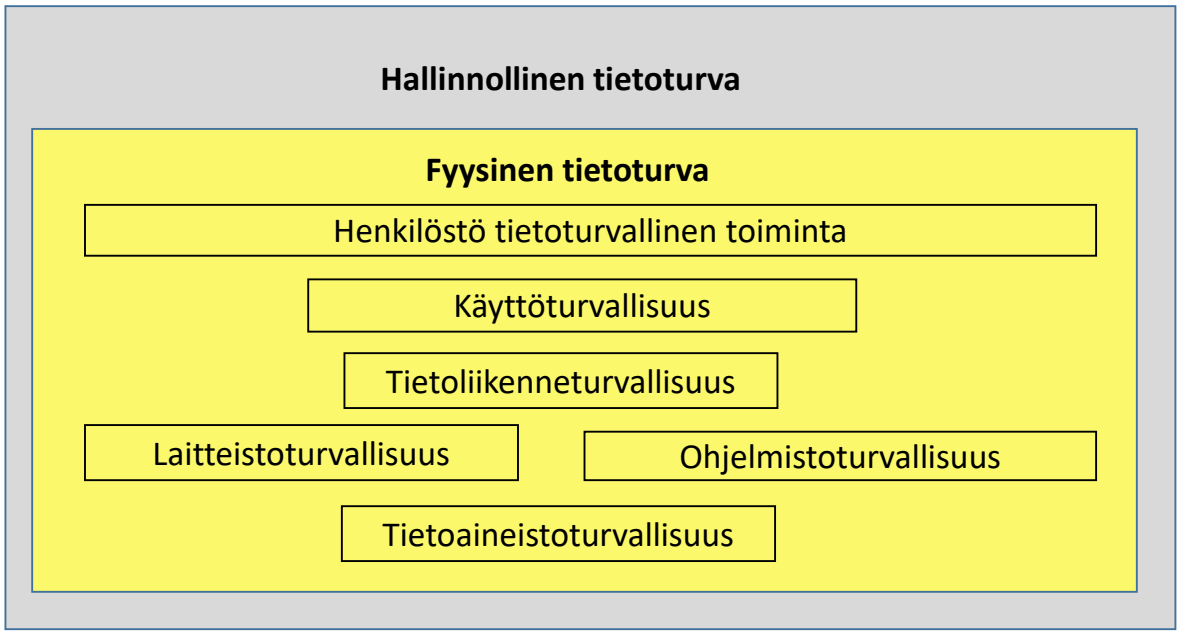
toteutetaan visio, eli unenomainen näky toiminnasta hamassa tulevaisuudessa), sekä toiminnan ohjaamisen periaatteet. Johdon tärkein asia on saattaa tietoturvalliset toimintatavat päivittäiseen toimintaan, osaksi prosesseja ja johtamista. Kuvioissa 1 on sovellettu Vastuullista liiketoimintaa tukevat johtamisjärjestelmät aineistoa sekä Hallinnollinen-turvallisuus dokumenteissa kuvattuja johtamisjärjestelmän kytköksiä. Kuviossa 1 on kuvattu miten visiosta johdetut strategiset tavoitteet ja tahtotila ohjaavat päivittäistä toimintaa. Politiikalla kuvataan tahtotilan periaatteet ja merkitykset.

Kuvio 1. Tietoturvan johto ja hallinta (Valtiovarainministeriö 2004 sekä Haaga-Helia).

Kuvion 1 mukaan johtaminen on tehtävien ja vastuiden jakamista, siten että asetetut tavoitteet voidaan saavuttaa. Koulutus tai toisilta nimiltään jalkautus tai maastouttaminen varmistaa, että annetut tehtävät voidaan suorittaa siten, että haluttu päämäärä saavutetaan. Päivittäiseen toimintaan kuuluvat prosessien hoitaminen, viestintä, ja seuranta, jotta mahdollisiin ongelmakohtiin voidaan puuttua riittävän ajoissa ja mielellään ennakkoon.

Vahti-ohjeen mukaan Hallinnollinen tietoturva sisältää myös ohjeet muiden tietoturvan osa-alueiden johtamista. Muita tietoturvan osa-alueita ovat: henkilöturvallisuus, fyysinen tietoturva, tietoliikenneturvallisuus, laitteistoturvallisuus, ohjelmistoturvallisuus, tietoaineistoturvallisuus ja käyttöturvallisuus.

Kuviossa 2 on kuvattu perinteinen jaottelu tietoturvan osa-alueista. Kaaviosta selviää, että hallinnollinen tietoturva kattaa fyysiseen tietoturvaan liittyvät osa-alueet. Hallinnollisessa tietoturvassa luodaan periaatteet, jotka ohjaavat fyysistä tietoturvaa. Hallinnollista tietoturvaa on mm. ohjeistus ja käyttäjien antama sitoumus noudattaa annettuja ohjeita. Fyysiseen tietoturvaan kuuluvat henkilö-, käyttö-, tietoliikenne-, laitteisto-, ohjelmisto- ja tietoaineistoturvallisuudet. Fyysisessä tietoturvassa keskeistä on henkilöiden toiminta annettujen ohjeiden mukaisesti. Henkilöstön on raportoitava havaitsemistaan puutteista. Organisaatiossa on ryhdyttävä tarvittaviin toimenpiteisiin tietoturvan vaarantuessa. Tietoturva on niin vahvaa, kuin sen heikoin lenkki on. Usein heikoin lenkki on henkilöstö. Tietoturvaa voisi lähestyä myös liiketoimintaprosessien kautta. Euroopan unionin sisäisen turvallisuuden rahaston (ISF) määrittelee ohjelmaksi ja tavoitteeksi mm. rikollisuuden ehkäisyn ja torjunnan sekä yhteiskunnan turvallisuuden varmistamisen (Euroopan Unionin sisäasioiden rahastot).



Kuvio 2. Hallinnollinen tietoturva luo puitteet tietoturvalle
(Valtiovarainministeriö 2004 sekä Laakso M., 9).

Tietoturvan johtaminen edellyttää päätöksiä tavoitteista ja täsmällisesti määriteltyä tietoturvatasoa. Organisaation on pystyttävä mittaamaan ja analysoimaan tietoturvan taso säännöllisesti. Tämä asettaa vaatimuksia toteutettavissa olevien mittareiden määrittelyyn. Mittareiden tulee kertoa organisaation tietoturvatasosta siten, että tarvittavat johtopäätökset ja toimenpiteet ovat suoritettavissa. Mittaamisen tulee kohdistua tietoturvan kokonaisuuden kehittämiseen ja johtamiseen, ei yksittäiseen pistemäiseen mittaamiseen (Valtiovarainministeriö 2003, Johdanto).

Mittaamisen perusteella tehdyt ratkaisut tulee pystyä jäljittämään ja niiden perusteella tulee voida löytää perustelut tehdyille ratkaisuille. Mittaaminen on pitkän aikavälin kehityksen seurannan apuväline. Laadukas toiminta edellyttää tietoturvallista toimintaa, ja samalla tietoturvallinen toiminta parantaa laatua. Tietoturvan heikoin lenkki on usein ihminen ja inhimillinen virhe. Siksi henkilökunnan koulutus ja avoin vuorovaikutteinen viestintä ovat yksi avaintekijä tietoturvallisen toiminnan juurruttamisessa organisaatioon. Motivoitunut, asian ymmärtävä henkilöstö pystyy parhaiten jatkuvasti analysoimaan riskejä ja tekemään parannusehdotuksia. Henkilökunnan tulee tietää miten tietoturvallisuutta mitataan, miksi mitataan ja mitä seuraamuksia tietoturvallisuuden rikkomisesta seuraa. Havaittuihin puutteisiin ja rikkomuksiin tulee puuttua välittömästi. Tarvittaessa ohjeistusta, koulutusta ja toimintatapoja on muutettava ripeästi (Valtiovarainministeriö 2004).

2.3 Tiedon käsittelyn tietoturva

Tietoturvaan kuuluu käytännön toimenpiteet, joilla varmistetaan tietojen eheys, saatavuus, oikeellisuus sekä tietojen luottamuksellisuuden säilyttäminen. Tällaisia keinoja ovat mm. tietosuojavastaavan nimittäminen, ohjeistuksen laatiminen, henkilöstön koulutus, osaamisen testaaminen, käyttövaltuuksien myöntämiskäytännöt, tilojen turvaamiset (esim. lukitukset), valvonta, seuranta ja raportointikäytännöt (OpiTietosuojaa.fi).

Tietosuojalla tarkoitetaan suojaa, jolla varmistetaan henkilön yksityisyys, edut, oikeudet, vapaudet ja oikeusturva. Tietosuojan tavoitteena on suojata henkilön (tiedon kohteen) tiedot (OpiTietosuojaa.fi).

Taulukossa 1 on kuvattu tietoturvan keskeiset periaatteet: saatavuus, luottamuksellisuus, eheys, kiistämättömyys, todennus, pääsynvalvonta (Virtuaali amk). Joidenkin lähteiden mukaan keskeisiin periaatteisin kuuluvat: luottamuksellisuus, eheys, käytettävyys ja todentaminen (Helsingin Yliopisto, opiskelijan digitaidot). Mielestäni laajempi terminologia avaa tietoturvan käsitettä paremmin sellaiselle lukijalle, joka ei ole perehtynyt asiaan. Laajempaa terminologiaa puoltaa myös hallinnollisen tietoturvan antama viitekehys (kuvio 2) sekä ISO/IEC 27001 standardin tietoturvan johtamisjärjestelmän pääkohdat sekä tietosuoja-asetuksen artiklan 32 vaatimukset.

Taulukko 2-1. Tietoturvan periaatteet (Virtuaali amk)

Termi	**Merkitys**
Saatavuus (availibility)	Tieto on saatavilla, kun sitä tarvitaan. Saatavuutta voidaan parantaa riittävän tiedonsiirtokapasiteetin varaamisella.
Luottamuksellisuus (Confidentiality):	Vain oikeudet omaavat henkilöt voivat käsitellä tietoa. Luottamuksellisuutta voidaan lisätä tiedon salauksella ja pääsynhallinnalla.
Eheys (Integrity):	Tieto ei muutu tahottomasti tai hyökkäyksessä, tiedon sisäinen ja ulkoinen loogisuus ja paikkansapitävyys, tiedon säilyminen kokonaisuutena, tiedon muuttuminen havaitaan. Eheyttä voidaan parantaa tarkistussummilla, tarkistuskoodeilla ja digitaalisella allekirjoituksella.
Kiistämättömyys (Non-Repudiation)	Viestin lähettäjä ei voi kiistää lähettäneensä viestiä.

	Kiistämättömyyttä voidaan parantaa digitaalisella allekirjoituksella.
Todennus tai todentaminen (Authentication, autentikointi)	Käyttäjän identiteetin varmentaminen joko luonnolliseksi henkilöksi tai oikeushenkilöksi Todentamista voidaan parantaa digitaalisella allekirjoituksella ja muilla todennustavoilla
Pääsynvalvonta / tunnistus (Access control)	Henkilön liittäminen käyttäjätunnukseen, joka oikeuttaa pääsyn järjestelmään

2.4 Tietoturvan hallintajärjestelmä

Tietoturvallisuuden hallintamallin käyttöönotto esimerkiksi ISO/IEC 27001 (Inspecta) kertoo sidosryhmille (luottamushenkilöt, asiakkaat, viranomaiset, jne.) että organisaation kanssa on turvallista asioida ja että riskien hallintaan on kiinnitetty huomiota.

Standardi kattaa kaikki tietoturvan hallintajärjestelmän osa-alueet, joita ovat:

1. Kartoitetaan toimintaympäristö ja määritellään tietoturvan johtamisjärjestelmä
2. Tunnistetaan sidosryhmät ja niiden vaatimukset
3. Organisaatiossa hyväksytetään tietoturvallisuuden periaatteet ja tavoitteet
4. Arvioidaan riskit, kuvataan riskien käsittelyprosessi ja dokumentaation hallinta
5. Määritellään tehtävät ja vastuut tietoturvan hallitsemiseksi
6. Kehitetään osaamista ja henkilöstön tietoisuutta tietoturvasta
7. Suojataan tiedot, tilat, tietojärjestelmät ja laitteet
8. ”Tietokoneiden ja tietoliikenteen hallinta”
9. Luodaan prosessit tietojärjestelmien kehittämiseen ja ylläpitoon
10. Varmistutaan varajärjestelmien ja toipumissuunnitelmien olemassaolosta
11. Noudatetaan lainsäädäntöä

(Inspecta ISO/IEC 27001)

”Valtioneuvoston tietoturvallisuutta koskevassa periaatepäätöksessä (VNp 11.11.1999) todetaan, että viranomaisilla tulee olla tietoturvallisuuden hallintaa ja ohjausta varten ajantasainen tiedonkäsittelyn turvaamissuunnitelma, vahinkojen varalta toipumissuunnitelma ja poikkeusolojen varalta tiedonkäsittelyn valmiussuunnitelma.” (Valtiovarainministeriö 2003, 9).

Samaa periaatepäätöstä tulee kaikkien niiden organisaatioiden noudattaa, joiden tarkoitus on jatkaa toimintaa myös poikkeusoloissa. Tämä edellyttää, että organisaatio määrittelee

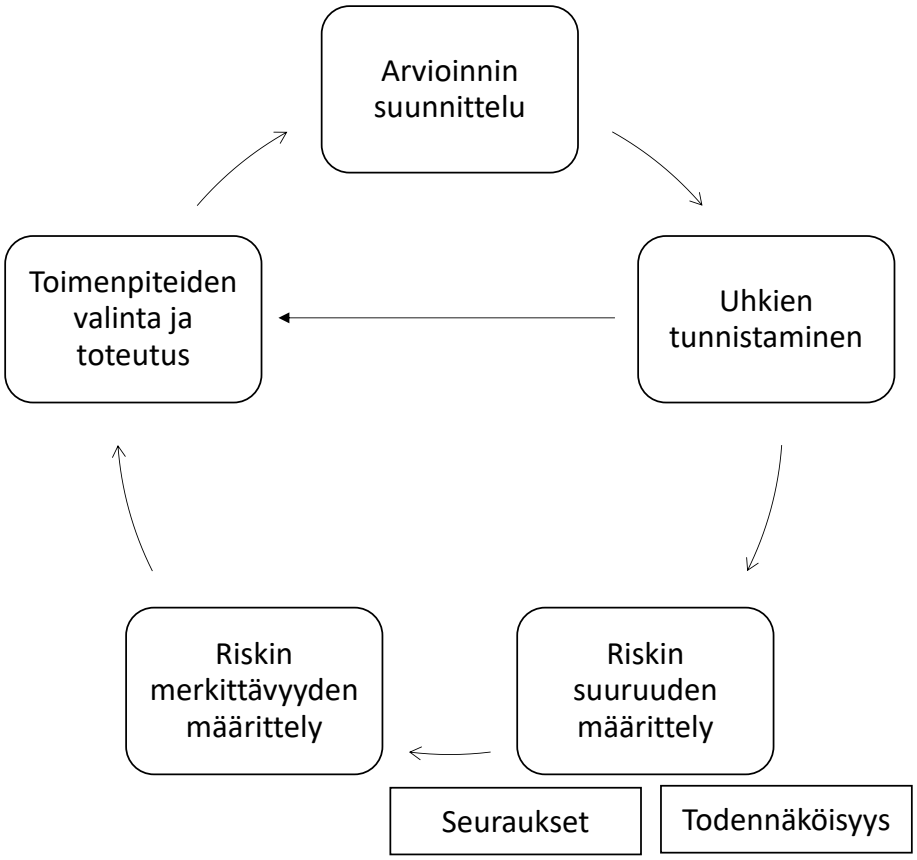
toimintaympäristönsä ja sen kautta tietoturvan hallintajärjestelmän kattavuuden (ISO/IEC 27001 standardissa: kohta 1) (Inspecta).

Tietoturvallisuuden hallinta on osa organisaation johtamisjärjestelmää, ei erillinen hallinnollinen tehtävä. (Valtiovarainministeriö 2003) Tietoturvan tulee olla luonteva osa päivittäistä toimintaa ja prosesseja, johdon esimerkki on ratkaisevaa, kuten keisari Augustukselle aikanaan sanottiin: *”Me emme tarvitse niinkään paljon hallitsijan käskyjä kuin hänen esimerkkiään”*. (Grimberg 1930, 4.osa, 291)

Johdon on tiedettävä organisaatioon toimintaan kohdistuvat toiminnan ja palveluiden asettamat tietoturvatarpeet ja vaatimukset. Johdon tulee arvioida ulkoiset ja sisäiset riskit sekä selvitettävä säädösten (laki) ja määräysten (asetukset ja muut määräykset) johtuvat tietoturvavaatimukset. Johdon on arvioitava toiminnan ja tietotekniikan muutosten vaikutukset tietoturvallisuuteen. Selvitettäviä asioita ovat myös sidosryhmien (asiakkaat, toimittajat, henkilöstö, yhteistyökumppanit, jne.) odotukset. (Inspecta).

Uhkien tunnistamisen ja riskien arvioinnin lähtökohtana tulee olla kriittinen ja ennakkoluuloton asenne. Uhkien ja riskien tarkastelun tulee olla kattavaa ja järjestelmällistä. Riskien ja uhkien tunnistaminen ja arviointi ovat prosesseja, joka voidaan kuvata seuraavasti (Valtiovarainministeriö 2003, 16):

Kuvion 3 mukaan uhkien ja riskien arviointi aloitetaan arviointiprosessin suunnittelulla. Seuraavaksi tunnistetaan karkealla menetelmällä uhat, jotta saadaan kokonaiskuva tilanteesta. Mikäli kyseessä on välitön uhka, niin toimenpiteet uhkan poistamiseksi aloitetaan välittömästi. Mikäli kyseessä on riski, joka ei aiheuta välitöntä vaaraa, arvioidaan riskin suuruus, todennäköisyys ja seuraukset. Tämän jälkeen päätetään riskin merkittävyys. Riskin suuruuden, todennäköisyyden ja merkittävyyden jälkeen määritellään toimenpiteet, joilla riski poistetaan.



Kuvio 3. Uhkien ja riskien arvioinnin ja hallinnan vaiheet (Valtiovarainministeriö 2003, 16)

Ylläkuvatulla karkealla kartoitusmenetelmällä löydetään ne riskialueet, joita on syytä tarkastella myöhemmin yksityiskohtaisesti. Tietoturvapolitiikkaa ja periaatteita koskevat päätökset ja yksityiskohtaiset suunnitelmat tulee perustua riskianalyysista saatuihin tuloksiin (Valtiovarainministeriö 2003, 16).

3 EU:n tietosuoja-asetus - GDPR

EU:n tietosuoja-asetus koskee kaikkia organisaatioita, jotka käsittelevät henkilötietoja käsittelijöinä ja / tai rekisterinpitäjinä niin yksityisellä kuin julkisella sektorilla. Vaatimus on voimassa riippumatta miten paljon ja millä tavalla henkilötietoja käsitellään. Asetusta sovelletaan määritellyissä tilanteissa myös EU:n rajojen ulkopuolella toimiviin organisaatioihin. Tietosuoja-asetusta sovelletaan sekä yksittäiseen henkilötietojen käsittelyyn että silloin kun henkilötiedot muodostavat rekisterin. Asetus tulee voimaan 25.5.2018. (Oikeusministeriö 2017, 9).

EU:ssa luonnollisten henkilöiden henkilötietojen suojelu on perusoikeus. Tietosuoja-asetuksen tarkoituksena on kehittää talousunionia, lujittaa talouksia, lähentää sisämarkkinoita sekä parantaa henkilöiden hyvinvointia (EU:n perusoikeuskirja, 8 artikla).

Henkilötietojen käsittely on suunniteltava siten, että se palvelee ihmistä. Henkilötietojen käsittelyn on oltava oikeassa suhteessa muihin EU:n perusoikeuksiin.
(Tietosuoja-asetus 679/2016/EU, (4))

Tietosuoja-asetus ei koske henkilökohtaista tai kotitalouden toimintaa (esimerkiksi joulukortit tai muu verkostoituminen). Asetus koskee kuitenkin niitä rekisterinpitäjiä, jotka tarjoavat keinot rekisterin ylläpitämiseen. Asetus ei koske kuolleita henkilöitä eikä anonyymien (yksittäisen henkilön henkilötiedot eivät ole tunnistettavissa, esim. tilastointi- tai tutkimustarkoitus) henkilötietoja. (Tietosuoja-asetus 679/2016/EU (18))

EU:n tietosuojadirektiivi puolestaan koskee toimivaltaisten viranomaisten tekemää henkilötietojen käsittelyä. Tällaisen käsittelyn tarkoituksena on rikosten ennaltaehkäiseminen, tutkiminen, paljastaminen tai syytetoimiin tai seuraamusten täytäntöönpanoon liittyvät tehtävät. Lisäksi direktiivin tarkoitus on yleisen turvallisuuden uhkien torjunta, ehkäisy ja suojelu (Tietosuojadirektiivi 680/2016/EU).

3.1 Käsitteistöä, artikla 4

Tietosuoja-asetuksen käsitteistö on kuvattu tietosuoja-asetuksen 4 artiklassa.
(Tietosuoja-asetus 679/2016/EU, 4 artikla)

Henkilötiedot: Henkilötiedoilla tarkoitetaan kaikkia niitä tietoja, joilla yksittäinen luonnollinen henkilö voidaan tunnistaa joko suoraan tai epäsuorasti. Henkilötietoja ovat esimer-

kiksi nimi, henkilötunnus, sormenjäljen kuva, lempinimi, rekisteritunnus, osoite, verkkotunnistetieto, biometrinentieto tai sijaintitieto. Henkilötietoihin kuuluu myös yhden tai usean henkilölle tunnusomaisen kulttuurisen, sosiaalisen, taloudellisen, geneettisen, psyykkisen, fysiologisen tai fyysisen tekijän ominaisuuden perusteella mahdollisesti tapahtuva tunnistaminen.

Biometrinen tieto: Niitä tietoja, joilla luonnollisen henkilön fyysisiin ja fysiologisiin ominaisuuksiin, käyttäytymiseen tai tekniseen käsittelyyn liittyviä tietoja joiden perusteella henkilö voidaan tunnistaa tai henkilön tunnistus voidaan varmentaa. Esimerkiksi kasvokuva, sormenjälki.

Geneettinen tieto: Luonnollisen henkilön geneettisiä ominaisuuksia, jotka on saatu perimällä tai hankkimalla. Tieto, jonka avulla saadaan selville tietoa henkilön fysiologiasta tai terveydentilasta. Tietoa, joka on saatu analysoimalla kyseisen henkilön biologista näytettä.

Terveystieto: Tietoja, jotka ilmaisevat henkilön fyysisen tai psyykkisen terveydentilan, myös tieto terveyspalvelun tarjoamisesta.

Henkilötietojen käsittely: Kaikki henkilötietoihin liittyvät toimenpiteet, kuten henkilötietojen kerääminen, tallentaminen, järjestäminen, päivittäminen, yhdistäminen, suojaaminen, käyttö, haku, kysely, siirto, rajoittaminen, luovuttaminen, levittäminen, säilytys, poistaminen ja tuhoaminen. Myös tietojen yhteensovittaminen tai yhdistäminen ovat henkilötietojen käsittelyä.

Profilointi: Etsitään henkilötietojoukosta ennakkoon määriteltyjä piirteitä, jotka yhdistävät eri-ihmisiä. Profiloinnin apuna voidaan käyttää henkilön käyttäytymistä, sijaintia, kiinnostuksen kohteita, taloudellista asemaa, terveydentilaa, henkilökohtaisia mieltymyksiä, työsuoritusta tai muuta henkilön luonnekuvaa.

Pseudonymisoiminen: Henkilötiedot käsittely siten, että henkilötietoa ei voida yhdistää yksittäiseen henkilöön käyttämättä lisätietoja. Pseudonymisoimisen edellytyksenä on, että lisätietoja säilytetään erillään. Lisäksi tulee varmistaa teknisin ja organisaation toimenpitein ettei yksittäisen henkilön tunnistamista suoriteta.

Rekisteröity: Henkilö, jonka henkilötietoja käsitellään.

Rekisteri: Mikä tahansa jäsennelty henkilötietoja sisältävä tietojoukko, josta henkilötiedot ovat saatavilla tietyin perustein. Rekisteri voi olla keskitetty tai hajautettu. Rekisteri voi olla jaettu toiminnallisin tai maantieteellisin perustein.

Rekisterinpitäjä: Luonnollinen tai oikeushenkilö (organisaatio), joka yksin tai yhdessä toisten kanssa määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot. EU tai jäsenvaltio voi määrittää lainsäädännöllä rekisterille / rekisterinpitäjälle erityiset tarkoitukset ja keinot.

Henkilötietojen käsittelijä: rekisterinpitäjän puolesta henkilötietoja käsittelevä henkilö, joka voi olla yksittäinen ihminen tai oikeushenkilö.

Vastaanottaja: henkilö (luonnollinen tai oikeus), joka vastaanottaa luovutettuja henkilötietoja. Viranomainen joka saa henkilötietoja lainsäädännön perusteella tai tutkimustarkoituksiin ei ole vastaanottaja.

Kolmas osapuoli / sivullinen: Muu kuin rekisterinpitäjä tai henkilötietojen kerääjä tai heidän lukuunsa henkilötietoja käsittelevä organisaatio tai henkilö, joka käyttää tai käsittelee henkilötietoja.

Rekisteröidyn suostumus: mikä tahansa vapaaehtoinen, yksilöity, tietoinen ja yksiselitteinen tahdonilmaisu tai lausuma tai selkeäsi suostumusta ilmaiseva toimi, jolla rekisteröitävä henkilö hyväksyy henkilötietojensa käsittelyn

Henkilötietojen tietoturvaloukkaus: toimenpide, jonka seurauksena vahingossa tai lainvastaisesti tuhotaan, hävitetään, muutetaan tietoja. Tietoturvaloukkaus on myös tietojen luovuttaminen ilman lupaa tai luvaton pääsy tietoihin.

Tietosuojavastaava: Seurakunnan (viranomaisen / julkishallinnon elimen) pitää nimittää tietosuojavastaava. Tietosuojavastaavan tulee olla organisaatiossa riippumattomassa asemassa, hän on raportointivelvollinen ylimmälle johdolle. Tietosuojavastaavalla tulee olla riittävä osaaminen ja tarvittavat resurssit. Tietosuojavastaava voi olla usean organisaation yhteinen.

Osoitusvelvollisuus: Organisaatiolla on velvollisuus näyttää toteen, että henkilötietojen käsittelyssä noudatetaan seuraavia periaatteita: 1. lainmukaisuus, kohtuullisuus ja läpinäkyvyys 2. käyttötarkoitussidonnaisuus, 3. tietojen minimointi, 4. täsmällisyys, 5. säilytysajan rajaaminen, 6. henkilötietojen eheys ja luottamuksellisuus.

Edustaja: EU:n alueelle sijoittautunut toimija, luonnollinen tai oikeushenkilö, joka käsittelee henkilötietoja toisen puolesta. Henkilötietojen käsittelypyyntö tulee tehdä kirjallisesti.

Henkilötietojen käyttö: Rekisterinpitäjä on kerännyt henkilötietoja määriteltyyn (määriteltyihin) käyttötarkoituksiin ja käyttää kerättyjä henkilötietoja omassa toiminnassaan. (OpiTietosuojaa.fi).

3.2 Henkilötietojen käsittelyä koskevat periaatteet, artikla 5

EU:n yleisen tietosuoja-asetuksen artiklassa 5 määritellään henkilötietojen käsittelyä koskevat periaatteet seuraavasti (Tietosuoja-asetus 679/2016/EU, 5 artikla):

Henkilötietoja on käsiteltävä lain- ja asianmukaisesti. Rekisteröidyn henkilön näkökannalta tietoja on käsiteltävä läpinäkyvästi. Käsittelyssä on noudatettava **lainmukaisuutta, kohtuullisuutta ja läpinäkyvyyttä**. Henkilötietoja saa kerätä määriteltyä laillista tarkoitusta varten **käyttötarkoitussidonnaisuus** huomioiden. Kerättyjen henkilötietojen tulee olla asianmukaisia ja olennaisia, ja niiden tulee olla rajoitettuja käyttötarkoitustaan varten eli tietojen määrä tulee **minimoida**.

Henkilötietojen tulee olla **täsmällisiä** ja niitä on tarvittaessa päivitettävä. Epätarkat ja virheelliset henkilötiedot tulee poistaa tai oikaista viipymättä. Korjaamisen ja oikaisujen suorittamiseksi on tehtävä kaikki kohtuulliset toimenpiteet huomioiden tekniset ja taloudelliset mahdollisuudet (Tietosuoja-asetus 679/2016/EU, 5 artikla).

Artikla 5 **rajoittaa henkilötietojen säilyttämistä**. Henkilötietoja saa säilyttää niin kauan kuin määritellyn tarpeen toteuttaminen vaatii. Henkilötiedot on säilytettävä sellaisessa muodossa, että henkilö on tunnistettavissa vain käyttötarkoitusta varten. (Tietosuoja-asetus 679/2016/EU, 5 artikla).

3.2.1 Henkilötietojen käsittely on sallittua

Artiklan 6 (Tietosuoja-asetus 679/2016/EU, 6 artikla)
mukaan lainmukaisuus täyttyy vain, jos vähintään yksi seuraavista edellytyksistä täyttyy:

a) Rekisteröity antaa suostumuksen henkilötietojensa käsittelyyn
b) Henkilötietojen rekisteröinti on tarpeen sopimuksen täytäntöön panemiseksi tai sopimuksen tekeminen edellyttää toimenpiteitä, joissa tarvitaan henkilötietoja. Edellytyksenä on, että rekisteröity pyytää sopimuksen tekoa.

c) Rekisterinpitäjän lainsäädännölliset velvoitteet edellyttävät henkilötietojen käsittelyä
d) Henkilötietojen rekisteröinti on välttämätöntä toisen luonnollisen henkilön elintärkeiden etujen suojaamiseksi
e) Mikäli tehtävä on suoritettava yleisen edun vuoksi tai rekisterinpitäjä hoitaa julkista valtaa
f) Mikäli rekisterinpitäjän tai jonkun muun toimijan oikeutettujen etujen toteuttaminen vaatii henkilötietojen käsittelyä.
   Rekisteröinti ei ole sallittua, mikäli rekisteröidyn edut, perusoikeudet ja -vapaudet syrjäyttävät rekisterinpitäjän edut. Mikäli kyseessä on lapsi, tulee rekisteröinnin oikeutus pohtia tarkkaan.

3.2.2 Henkilötietojen käsittely on kiellettyä

Kiellettyä on käsitellä tietoa, joka liittyy rotuun, etniseen alkuperään, poliittiseen mielipiteeseen, uskonnolliseen tai filosofiseen vakaumukseen ja ammattiliiton jäsenyyteen. Henkilön tunnistamista varten kerättävä geneettinen tai biologinen tieto on kielletty. Myös terveyteen, seksuaaliseen käyttäytymiseen ja suuntautumiseen liittyvän tiedon käsittely on kielletty (Tietosuoja-asetus 679/2016/EU, 9 artikla).

Kerättyjä tietoja ei saa myöhemmin käyttää alkuperäisen tarkoituksen kanssa yhteensopimattomalla tavalla. Yleisen edun mukainen arkistointi tai tieteellinen tai historiallinen tutkimustarkoitus tai tilastointi ei ole yhteensopimatonta (Tietosuoja-asetus 679/2016/EU, 5 artikla).

3.3 Suostumus, artikla 7

Henkilötietojen käsittely voi perustua rekisteröidyn henkilön antamaan suostumukseen. Rekisterinpitäjän on voitava osoittaa, että on saanut rekisteröidyn suostumuksen. Kirjallinen suostumus on esitettävä selkeästi ja erillään muusta asioinnista tai asioista, suostumuslomakkeen on oltava selkeä ja yksinkertaisesti kirjoitettu. Monimutkainen epäselvästi kirjoitettu suostumus ei ole pätevä (Tietosuoja-asetus 679/2016/EU, 7 artikla).

Rekisteröidyllä henkilöllä on oikeus perua suostumus milloin tahansa. Ennen suostumuksen peruutusta käsittely on lainmukaista, mikäli muut ehdot täyttyvät. Suostumuksen peruutuksen tulee olla yhtä helppoa kuin suostumuksen antaminen. Suostumuksessa voidaan pyytää sellaisia henkilötietoja, jotka ovat sopimuksen teon kannalta tarpeellisia (Tietosuoja-asetus 679/2016/EU, 7 artikla). Lapsen suostumusta käsitellään Tietoturva-asetuksen 8 artiklassa. Artiklan mukaan yli 16-vuotiaan lapsen henkilötietojen käsittely on

lainmukaista. Alla 16-vuotiaan lapsen osalta tarvitaan huoltajan (vanhempainvastuunkantaja) suostumus (Tietosuoja-asetus 679/2016/EU, 8 artikla).

3.4 Rekisteröidyn oikeudet

Rekisteröidyn oikeuksiin otetaan kantaa Tietosuoja-asetuksen III luvussa. Artiklassa 12 otetaan kantaa läpinäkyvyyteen informoinnissa ja viestinnässä. Rekisteröidyn tulee saada kaikki henkilötietojen käsittelyyn liittyvä tieto helposti ymmärrettävässä muodossa ja selväkielisesti. Tietojen antaminen suullisesti edellyttää, että rekisteröidyn henkilöllisyys on vahvistettu ennen tietojen luovuttamista (Tietosuoja-asetus 679/2016/EU, 12 artikla).

Artikla 15 takaa rekisteröidylle oikeuden saada tietoa omien henkilötietojen käsittelystä. Rekisteröidylle tulee ilmoittaa käsitelläänkö hänen henkilötietojaan vai ei. Mikäli henkilötietoja käsitellään, niin rekisteröidyllä on oikeus päästä seuraaviin tietoihin: käsittelyn tarkoitus, henkilötietoryhmät, henkilötietojen vastaanottajat ja vastaanottajaryhmät erityisesti kansainväliset käsittelijät, suunniteltu säilytysaika ja ajan määrittämisen perusteet, oikeus omien henkilötietojen oikaisemiseen tai poistamiseen tai käsittelyn rajoittamiseen, oikeus valituksen tekemiseen valvontaviranomaiselle. Sillä ei ole merkitystä onko tieto kerätty rekisteröidyltä itseltään vai onko tieto saatu joistain muualta.

Rekisteröidyn on saatava tietää automaattisen päätöksentekoon liittyvä profilointi ja profiloinnin perusteella oleva logiikka sekä näistä johtuvat seuraamukset. Artikla 16 takaa rekisteröidylle oikeuden saada oikaistua omat virheelliset, puutteelliset tai epätarkat tietonsa. Artikla 17 takaa oikeuden tulla unohdetuksi, mikäli rekisterinpitäjä ei tarvitse enää tietoja kerättyä tarkoitusta varten, tai rekisteröity peruuttaa suostumuksen eikä käsittelyyn ole laillista perustetta. Rekisteröity voi vastustaa henkilötietojensa käsittelyä esimerkiksi suoramarkkinoinnissa tai profiloinnissa. Profilointia voidaan käyttää, mikäli rekisterinpitäjä pystyy osoittamaan, että profiloinnilla on perusteltu ja huomattavan tärkeä syy.

3.5 Rekisterinpitäjä ja henkilötietojen käsittelijä

Henkilötietojen suojaamiseksi rekisterinpitäjän ja henkilötietojen käsittelijän on toteutettava asianmukaiset tekniset ja organisatoriset toimenpiteet. Tarvittavien toimenpiteiden määrittelyyn vaikuttavat mm. uusin tekniikka ja sen toteuttamiskustannukset sekä henkilötietojen käsittelyn luonne, laajuus ja tarkoitus. Toimenpiteiden määrittelyssä on otettava huomioon myös riskien todennäköisyys ja vakavuus. Rekisterinpitäjän on osoitettava, että näitä velvollisuuksia noudatetaan (Tietosuoja-asetus 679/2016/EU, 24 artikla).

Artiklan 25 kohdan 1 mukaan rekisterinpitäjän on määritelleessään ja käyttäessään henkilötietoja otettava huomioon uusimmat tekniset mahdollisuudet rekisteröityjen oikeuksien suojaamisessa. Riskien vakavuus ja todennäköisyys on otettava huomioon, kun pohditaan tarvittavien toimenpiteiden kustannusvaikutuksia (Tietosuoja-asetus 679/2016/EU, 25 artikla).

Kohdassa 2 todetaan: *”Rekisterinpitäjän on toteutettava asianmukaiset tekniset ja organisatoriset toimenpiteet, joilla varmistetaan, että oletusarvoisesti käsitellään vain tarkoituksen kannalta olennaisia tietoja”.* Rekisterinpitäjän on varmistettava, että henkilötietoja pääsee käsittelemään vain valtuutetut henkilöt (Tietosuoja-asetus 679/2016/EU, 25 artikla).

Artikla 42 määrittelee sertifiointimekanismit, joiden avulla voidaan osoittaa että 25 artiklan kohtia 1 ja 2 vaatimuksia noudatetaan (kustannukset huomioiden on toteutettava kaikki tekniset ja toiminnalliset toimenpiteet tietojen minimoimiseksi ja suojaamiseksi). Artikla 32 määrittää henkilötietojen käsittelyn turvallisuuteen liittyvät asiat, joita ovat a) henkilötietojen pseudonymisointi ja salaus; b) järjestelmien ja palveluiden luottamuksellisuus, eheys, käytettävyys ja vikasietoisuus; c) kyky palauttaa nopeasti tietojen saatavuus ja pääsy tietoihin fyysisen tai teknisen vian sattuessa; d) menettely, jolla testataan, tutkitaan ja arvioidaan säännöllisesti teknisten ja organisatoristen toimenpiteiden tehokkuutta tietojenkäsittelyn turvallisuuden varmistamiseksi (Tietosuoja-asetus 679/2016/EU).

4 Seurakunnan tiedonhallinnan valmistelu EU tietosuoja-asetuksen käyttöönottoon

4.1 Projektisuunnitelma

Empiirisen osan tavoitteena on tehdä valmistelevat toimenpiteet EU:n tietoturvadirektiivin huomioimiseksi. Tietosuoja-asetuksen voimaantulossa on kyse ennemmin prosessien muuttumisesta, kuin kertaluonteisesta projektista. Ensimmäisenä vaiheena tarvitaan projekti, joka käynnistää prosessin. Valtiovarainministeriön suositukset tarvittavista toimenpiteistä löytyvät Vahti-raportin 1/2016 kohdasta 6. Raportin mukaan päävaiheita ovat: 1) Johdon tahtotilan ilmaisu. 2) Ohjeistus ja koulutus 3) Kehittäminen. 4) Seuranta ja raportointi. (Valtiovarainministeriö 2016b, 31).

Tietosuoja-asetuksen mukaan rekisterinpitäjän tulee varmistaa henkilötietoturvallisuus tietojen elinkaaren ajan. Tietosuojavastaavan on raportoitava säännöllisesti sekä virkamiesjohdolle että kirkkoneuvostolle / yhteiselle kirkkoneuvostolle tietosuojan tilanteesta. Yksi tapa on vuosittain tehtävä tietotilinpäätös. Kirkossa tietosuojavastaava voi olla seurakunnan tai seurakuntayhtymän palveluksessa, it-alueen yhteinen tai muuten seurakuntien puolesta yhteisesti toimiva henkilö (Kirkkohallituksen yleiskirje 6/2017).

Kuviosta 4 on nähtävissä, että seurakunnan johdon (virkamies ja luottamushenkilöt) on määriteltävä seurakunnan tahtotila (**Johdon tahtotila**), joka ohjaa päivittäistä toimintaa, toimintatapojen kehittämistä ja uusien tietoteknisten järjestelmien käyttöönottoa. Tavoitteiden saavuttamiseksi tulee varata riittävät resurssit, seurata projektin ja prosessin etenemistä sekä ohjattava, tuettava ja annettava riittävät resurssit tietosuoja-asetuksen vaatimien käytännön toimenpiteiden suorittamiseksi. Tarvittaessa tehtäviä on priorisoitava (Valtiovarainministeriö 2016b, 31)

Kuvio 4. Tietosuoja-asetuksen prosessi (Valtiovarainministeriö 2016b, 31).

Kuvion 4 mukaan henkilöstö, yhteistyötahot ja luottamushenkilöt on koulutettava ja ohjeistettava (**Ohjeistus ja koulutus**). Luottamushenkilöjohdon rooliin kuuluu ohjeistaa ja valvoa viranhaltijoita ja työntekijöitä, päätöksiä tehdessään luottamushenkilöt (neuvosto) ovat usein myös henkilötietojen käsittelijöitä. Riittävän tietosuoja- ja tietoturvaosaamisen varmistamiseksi tulee järjestää tarvittavia tietosuojakoulutuksia (Valtiovarainministeriö 2016b).

Tietosuoja-asetuksen empiirinen osa (**Analyysit ja kehittäminen**) toteutetaan projektina, jonka päävaiheet ovat rekistereiden kartoitus, arviointi, dokumentointi ja ylläpidon sekä kehittämiskohteiden määrittely (Valtiovarainministeriö 2016b, 33).

Kuviosta 4 nähdään, että prosessin viimeinen vaihe on **seuranta & raportointi.** Johdon tulee pystyä näyttämään toteen osoitusvelvollisuuden toteutuminen (tietoja käsitellään lain- ja tarkoituksenmukaisesti, täsmällisesti ja luotettavasti). Tietosuojavastaavan tulee raportoida johdolle säännöllisesti käytetyistä tietosuojamittareista, kehittämishankkeista, puutteista ja tarpeista, tietoturvaloukkauksista, riskien ja vaikutustenarviointien löydöksistä sekä niiden hallintakeinoista, rekisteröityjen oikeuksien toteutumisesta ja yhteistyöstä valvontaviranomaisten kanssa (Valtiovarainministeriö 2016b, 36).

4.2 Johdon tahtotila

Kirkkoherran ja talous-/hallintojohdon osallistuminen ja tuki tietosuojatyölle on yksi onnistumisen peruspilareista. Sekä virkamies- että luottamushenkilöjohdon on varmistetta, että

tietosuojan nykytilan arviointiin ja tarvittavien toimenpiteiden suorittamiseen on käytettävissä tarvittavat resurssit. Sekä virkamies- että luottamushenkilöjohdon on jatkossa seurattava tietosuojan tilannetta säännöllisesti. Tietosuojavastaavan raportointi johdolle on osa osoitusvelvollisuuden täyttymistä. Vuoden 2018 toimintasuunnitelmassa ja talousarviossa on syytä varautua tietosuoja-asetuksen voimaantuloon. Johdon on tiedettävä missä ollaan, jotta se voi määritellä reitin tulevaan.

Tietosuojaa ohjaavat periaatteet voidaan kirjoittaa yhteen dokumenttiin, jossa kuvataan tietosuojapolitiikan lisäksi tietoturvapolitiikka ja tietoturvamääräykset. Dokumentoitavia asioita ovat myös seloste käsittelytoimista, tietosuojaselosteet, ohjeet henkilötietojen käsittelemiseksi, prosessikaaviot rekisteröityjen oikeuksista, tietotilinpäätökseen liittyvä sisäinen ja ulkoinen viestintä, kuvaus tietosuojatyön suunnittelusta ja seurannasta sekä tietosuojavastaavan päiväkirja. Liitteenä on Tietosuoja ja tietoturva Pornaisten seurakunnassa dokumentti, jossa asia on avattu (LIITE 1).

Seurakunnan it-toiminnot on ulkoistettu it-alueen hoitoon. It-alueiden perustamisvaiheessa tai kun seurakunta on liittynyt it-alueeseen, on määritelty tietosuojaan ja tietoturvaan liittyvät yleiset seurakunnille yhteiset periaatteet. Sitä vastoin rekisteri-/tietosuojaselosteet, kuvaus ja ohjeistus henkilötietojen käsittelyistä sekä riskienhallinnan periaatteet ovat seurakunnan vastuulla. Näiden periaatteiden dokumentointi on johdon vastuulla. Tässä työssä it-alueella kannattaa tehdä yhteistyötä siten, että it-alue tai Kirkkohallituksen it-yksikkö luo pohjadokumentin, jota seurakunta päivittää seurakuntakohtaisilla tiedoilla.

Johdon tulee varmistaa, että tietosuoja on otettu huomioon seurakunnan erilaisissa suunnitelmissa, joita ovat mm. valmius-, viestintä- ja toimintasuunnitelmat. Seurakunnat voivat nimittää yhteisen tietosuojavastaan. Töitä on tarvittaessa organisoitava uudelleen ja yhteistyötä yli seurakuntarajojen on haettava aktiivisesti. Tietosuojavastaavan nimeämisessä on varmistettava, että valittavalla henkilöllä on riittävä osaaminen, valtuudet ja resurssit tehtävän hoitamiseen. Riippumattomuuden varmistamiseksi tietosuojavastaavan asema organisaatiossa on pohdittava tarkoin. Kirkon yleisten tietoturvamääräysten mukaan tietoturvaryhmä ja tietosuojavastaava ovat IT-aluekohtaisia. Seurakunnan tulee nimetä tietoturvan yhdyshenkilö. (Kirkkohallitus 2016). Tietosuojavastaava sekä tietosuojayhteyshenkilö tulee nimetä mahdollisimman varhaisessa vaiheessa, jotta valitut henkilöt voivat ohjata työtä heti sen alkuhetkistä lähtien.

4.3 Ohjeistus ja koulutus

Satsaaminen henkilökunnan koulutukseen on yksi esimerkki johdon sitoutumisesta. Ohjeistuksen ja koulutuksen tarkoituksena on varmistaa, että henkilökunta osaa toimia sekä normaali että kriisitilanteissa tarkoituksenmukaisella tavalla. Ohjeistuksissa ja koulutuksissa kannattaa hyödyntää yleisiä avoimia lähteitä kuten Juhta-Vahti yhteishankkeiden materiaaleja, Arjen tietosuojan koulutusaineistoaja ja Kirkkohallituksen sekä it-alueiden ohjeistuksia ja koulutuksia. Koulutusta on annettava henkilöstölle sekä niille luottamushenkilöille ja vapaaehtoisille, jotka käsittelevät henkilötietoja. Henkilöstön koulutuksella tarkoitan koulutusta, joka annetaan sekä henkilökunnalle että luottamushenkilöille. Esimieskoulutus on koulutus, jota annetaan organisaation vastuuhenkilöille.

Pienen seurakunnan tietosuojapolitiikan voi kiteyttää seuraavasti: Pornaisten seurakunta noudattaa EU:n tietosuoja-asetuksen ja kansallisen lainsäädännön asettamia rekisterinpitäjän velvollisuuksia. Kaikessa toiminnassa otetaan huomioon rekisteröityjen oikeudet. Tietosuojasta vastaa talouspäällikkö yhdessä kirkkoherran ja kirkkoneuvoston kanssa. Talouspäällikkö toimii tietosuoja-asioissa asiantuntijana ja yhteyshenkilönä.

Tietoturvapolitiikassa ja tietoturvamääräyksissä noudatetaan Kirkkohallituksen ja kirkolliskokouksen määräyksiä ja ohjeistuksia sekä IT-alueen antamia soveltamisohjeita. Henkilöstö, luottamushenkilöt, vapaaehtoiset ja muut toimijat jotka työssään tai luottamustoimessa käsittelevät henkilötietoja allekirjoittavat salassapitosopimuksen. Tietoturvan yhdyshenkilön tehtävänä on tiedottaa ohjeista, suosituksista ja määräyksistä seurakunnan eri toimijoille. Liitteenä on Pornaisten seurakunnan tietoturvaa- ja tietosuojaa ohjaava dokumentaatio sekä esimerkkejä muista dokumenteista (Liite 1).

Henkilöstön koulutuksissa tulee käsitellä ainakin tietosuojan perusteet. Koulutuksessa tulee näyttää esimerkein mistä on kyse, kun puhutaan tietosuojan tai tietoturvan pettämisestä. Koulutuksessa tulee käsitellä myös miten toimitaan poikkeustilanteissa, mikä on jokaisen henkilötietoja käsittelevän vastuu ja velvollisuus. Koulutuksen jälkeen henkilöstön ja henkilötietoja käsittelevien luottamushenkilöiden tulee tiedostaa, että tietosuoja on jokaisen perusoikeus. Henkilötietojen käsittelyllä tulee olla lakiin, henkilönsuostumukseen tai asiakkuuteen perustuva oikeutus. Koulutuksessa on syytä käydä tiivisti läpi EU:n tietosuoja-asetuksen ydinkohdat. Koulutuksessa tulee selkeyttää keskeisten termien sisältöä, tällaisia termejä ovat: henkilötiedot, arkaluontoinen henkilötieto, henkilörekisteri, rekisterinpitäjä, henkilötietojen käsittelijä, suostumus ja rekisteriseloste. Koulutuksen lopuksi on hyvä järjestää testi, jonka perusteella henkilölle voidaan myöntää todistus osaamisesta. Todistus on yksi keino seurakunnan osoitusvelvollisuuden toteennäyttämisessä.

Johdon ja esimiesten koulutuksissa tulee käsitellä ainakin EU:n tietosuoja-asetuksen tavoitteet, keskeisten termien kertaus, tietoturva ja tietosuoja, tietosuoja-asetuksen velvoitteet seurakunnalle rekisterinpitäjänä, johdon roolin merkitys, johdon vastuu, tiedon elinkaari, rekisteröidyn oikeudet, riskienhallinta, tietoturvan pettäminen, tietosuojavastaavan tehtävät ja asema, tietosuoja hankinnoissa ja sopimuksissa, osoitusvelvollisuus, tietosuoja- ja tietoturvadokumentaatio, valvonta- ja seurantavelvollisuus, vinkkejä käytännön toimintaan ja hallinnolliset seuraamukset tietosuojan pettäessä. Tässä vaiheessa on tarkistettava, että salassapitosopimukset (henkilöstö, muut henkilötietoja käsittelevät) ovat ajan tasalla. Myös muun dokumentaation ja ohjeistuksen ajantasaisuus ja olemassaolo tulee tarkistaa. Valtiohallinnon tieto- ja kyberturvallisuuskeskuksen (VAHTI) laatimat koulutusaineistot löytyvät osoitteesta: http://arjentietosuoja.fi

4.4 Analyysit ja kehittäminen

Suunnistamisessa on tärkeää tietää missä ollaan, jotta voidaan määritellä tarkoituksenmukainen reitti tavoitteeseen pääsemiseksi. Seurakunnan tulee tietää tietosuojan nykytila, jotta se voi laatia tarkoituksenmukaisen kehittämisohjelman tietosuoja-asetuksen velvoitteiden täyttämiseksi. Kysymys ei ole ainoastaan tekniikasta ja tietojärjestelmistä, vaan ennen kaikkea ihmisten toiminnasta ja asenteista. Kun tiedetään, missä ollaan ja mihin ollaan menossa, voidaan arvioida ja priorisoida tarvittavat toimenpiteet ja niiden vaikutus seurakunnan toimintaan ja talouteen. Koulutus ennen nykytila-analyysia luo tehtävälle merkityksen. Nykytila-analyysi keskeisiä vaiheita ovat: henkilörekistereiden kartoitus, sopimusten kartoitus ja henkilörekistereiden käsittelyn nykytilan analysointi. Kuvaan seuraavassa nämä vaiheet lyhyesti.

Nykytilan analysointi kannattaa aloittaa **kartoittamalla** seurakunnan käytössä olevat **henkilörekisterit**. Henkilörekistereiden kartoitusta varten on hyvä laatia taulukko, jossa sarakkeina tai riveinä ovat henkilörekisterin nimi / käyttötarkoitus, tietojen tallennustapa /-paikka (esim. Katrina, Excel, Status, Kipa, jne.), rekisterin vastuuhenkilö, pääkäyttäjä, käyttöoikeudet, miten rekisteri on suojattu, sopimuskumppanit, henkilötietoluokat, käsittelyperuste, säilytysaika, tietovirrat ja maantieteellinen sijainti.

Taulukko 4-1. Esimerkki kartoituksesta

Kartoituksen kohde	**Kartoituksen tulos**
Henkilörekisterin nimi / käyttötarkoitus	Status hautaustoimi
Tietojen tallennustapa /-paikka	Status ohjelmisto
Tietojen tallennuspaikka	Kirkkohallituksen palvelukeskus / CGI
Rekisterin vastuuhenkilö	Toimistonhoitaja
Pääkäyttäjä	Toimistonhoitaja
Käyttöoikeudet	Toimistonhoitaja, talouspäällikkö, hautausmaanhoitaja
Suojaus	Verkon käyttäjätunnus ja salasana Sovelluksen käyttäjätunnus ja salasana
Sopimuskumppanit	Kirkkohallitus, CGI Suomi Oy
Henkilötietoluokat	Arkaluonteinen henkilötieto
Käsittelyperuste	Hautaustoimen asiakkuus, sopimus omaisen kanssa
Säilytysaika	Sopimuksen voimassaoloaika + 5 vuotta
Tietovirrat	Paperituloste, siirto Exceliin
Maantieteellinen sijainti	Suomi
Muilla mahdollisesti rekisteriin pääsy	Kirkkohallituksen käyttötuki CGI:n sovelluskehitys
Huomioita	Salasana lukkiutuu x virheellisen salasanan jälkeen

On syytä huomata, että rotuun tai etniseen alkuperään, poliittiseen mielipiteeseen, uskonnolliseen tai filosofiseen vakaumukseen, ammattiliiton jäsenyyteen, terveyteen, seksuaaliseen suuntautumiseen tai käyttäytymiseen sekä geneettiseen tai biometrisen liittyvien tietojen käsittelyä varten tulee olla vahvat perusteet. Seurakunnan luottamushenkilörekisterissä ilmenee uskonnollinen ja poliittinen mielipide, koska henkilö on ilmaissut tiedon asettuessaan ehdolle vaaleihin. Ammattiliiton jäsenyys sekä terveyteen liittyvää tietoa löytyy todennäköisesti henkilöstöhallinnon järjestelmistä (ay-jäsenmaksujen perintä, sairauslomat). Näissä tilanteissa tiedon käsittely on sallittua.

Sopimusten **kartoittamisessa** tarkistetaan miten toimittajaa on ohjeistettu henkilörekistereiden käytön osalta. Huomaa, että ohjelmiston ylläpitäjä voi päästä henkilötietoihin. Tyypillinen arkaluontoista henkilötietoa sisältä ohjelmisto on Katrina-diakonia. Kipan ja Statuksen osalta otetaan yhteys Kirkkohallituksen tietohallintoyksikköön, jonka palveluita seurakunnan on pakko käyttää. Huomaa, että vastuu henkilörekisteristä on seurakunnalla, ei Kirkkohallituksella. Alla olevaan taulukkoon on poimittu henkilörekistereiden kartoituksessa esille nousseita sopimuskumppaneita sekä sopimusten kohteet, sen lisäksi taulukosta ilmenee miten henkilötietojen käsittely on ohjeistettu kyseisen sopimuksen yhteydessä. Tarvittaessa sopimuksia on muutettava ja täydennettävä.

Taulukko 4-2. Esimerkki sopimusten kartoituksesta

Sopimuskumppani	Sopimuksen kohde	Miten henkilötietojen käsittely on ohjeistettu
Kirkkohallitus	Status hautaustoimi, käytön tuki	Henkilötietoja käsittelevän on allekirjoitettava salassapitosopimus.
Kirkkohallitus / Kirkon palvelukeskus KIPA	Kipa talous- ja henkilöstöhallinnon tietojärjestelmät ja palvelut	Henkilötietoja käsittelevän on allekirjoitettava salassapitosopimus.
CGI Suomi Oy	Status, sovelluskehitys	Henkilötietoja käsittelevän on allekirjoitettava salassapitosopimus.
M&V Software	Katrina ohjelmisto	Henkilötietoja käsittelevän on allekirjoitettava salassapitosopimus.

Arvioi henkilötietojen käsittelyn nykytila **vertaamalla** nykytilaa tietosuoja-asetuksen vaatimuksiin, erityisesti rekisteröityjen oikeudet ja henkilötietojen käsittelyn riskit. Seurakunnalla on useita työalakohtaisia tai työntekijäkohtaisia rekistereitä, siksi arviointi suoritetaan työaloittain. Tätä vaihetta ohjaa EU:n tietosuoja-asetuksen artiklat 5 - 12.

Arvioinnissa on kiinnitettävä huomiota että henkilötietoja käsitellessä noudatetaan lainmukaisuutta, kohtuullisuutta, läpinäkyvyyttä, käyttötarkoituksenmukaisuutta, käsitellään vain tarvittavia henkilötietoja, huolehditaan että henkilötiedot ovat oikein ja täsmällisiä, henkilötietojen säilytys on rajoitettu käyttötarkoituksen mukaisesti sekä huolehditaan henkilötietojen turvallisuudesta ja suojaamisesta.

Arviointi aloitetaan kartoittamalla millä perusteella rekisteriä ylläpidetään. Mikäli kartoituksessa vastataan vähintään yhteen seuraavista kysymyksistä myönteisesti, löytyy perustelu tietosuoja-asetuksesta. Kartoita seuraavat asiat: onko asiakas / seurakuntalainen antanut yksiselitteisen suostumuksen, onko asiakkaan / seurakuntalainen kanssa solmittu sopimus, onko kyseessä rekisteröidyn (seurakuntalaisen) elintärkeä etu tai rekisterinpitäjän (seurakunnan) tai kolmannen osapuolen oikeutettu etu (esimerkiksi saatavan turvaaminen).

Mikäli edellä mainittuihin kysymyksiin ei löytynyt myönteistä vastausta, voi rekisterin pitämisen oikeutus löytyä kansallisesta laista. Näissä asioissa avainkysymyksiä ovat: perustuuko rekisterinpito lakisääteisten velvoitteiden hoitamiseen vai onko perusteluna yleisen tehtävän hoitaminen tai julkisen vallan käyttäminen.

Seuraavaksi arvioidaan käsitelläänkö rekisterissä erityisiä henkilötietoryhmiä, joita ovat mm. uskonnollinen vakaumus, terveyttä koskeva tieto, seksuaalista käyttäytymistä tai suuntautumista koskeva tieto tai ammattiliiton jäsenyys.

Nykytila-analyysin työkaluna voidaan käyttää Exceliä, jossa väreillä ilmaistaan rekisterin käsittelyn nykytila ja mahdolliset ongelmakohdat. Taulukosta 5 havaitaan että Status hautaustoimen henkilötietojen käsittelyyn on kiinnitettävä huomiota. Henkilötietojen oikeellisuudessa on puutteita, joka ilmenee taulukossa punaisena värinä. Keltainen väri ilmaisee, että tietojen säilytysajasta on epävarmuutta. Muut arvioinnin kohdat ovat vihreällä, eli näiden osalta rekisterin käsittely vastaa tietosuoja-asetuksen vaatimuksia.

Seuraava vaihe on analysoida organisaation yleinen ymmärrys tietosuojan valmiudesta ja ohjaavien dokumenttien kattavuudesta. Arvioitavia kohtia ovat: rekisteröityjen oikeuksien toteutuminen, rekisterinpitäjän velvollisuuksien toteutuminen sekä johdon toiminta. Arvioinnin teossa voi käyttää Valtiovarainministeriön JUHTA-VAHTI-yhteishankkeissa julkaistuja työkaluja.

Rekisteröityjen oikeuksien toteutumisessa arvioidaan seuraavien kriteerien perusteella: Onko seurakunta ymmärtänyt rekisterinpitäjän tiedonantovelvollisuuden? Onko seurakunta varmistanut rekisteröidyn oikeuden nähdä omat tietonsa? Onko rekisteröidyllä oikeus oikaista virheelliset tietonsa ja vaatia tulla unohdetuksi (tietojen poistovaatimus)? Miten seurakunnassa menetellään rekisteröidyn vaatiessa tietojen siirtoa toiseen järjestelmään? Rekisteröidyllä on oikeus tietää käyttääkö seurakunta profilointia tai automaattista päätöksentekoa.

Rekisterinpitäjän velvollisuuksien tilannetta kartoitetaan seuraavien näkökulmien kautta: Ymmärretäänkö seurakunnassa henkilötietojen käsittelyn oikeusperusta. Onko tietosuojan hallinnointi, roolit ja vastuut selvät. Onko seurakunta nimennyt tietosuojavastaavan ja onko hänen asemansa ja tehtävänkuvansa kunnossa. Minkälainen tietosuojaorganisaatio seurakunnalla on. Miten seurakunnassa toteutuu oletusarvoinen tietosuoja, onko tietojen käyttötarkoitus harkittua ja onko riskiarviot tehty. Miten tietosuoja toteutuu hankinnoissa ja projekteissa. Miten seurakunta huolehtii tietoturvallisuudesta. Onko riskienarviointi aktiivisessa käytössä. Miten fyysinen turvallisuus, henkilöturvallisuus, omaisuuden turva, tiedonhallinta, jatkuvuuden hallinta ja henkilötietojen käsittely on hoidettu. Täyttääkö seurakunnan dokumentaatio, ohjeistus ja sopimukset tietosuojavaatimukset. Miten poikkeamien käsittely toimii.

Taulukossa 4 nähdään henkilörekisterien nykytilakartoituksen tulos. Havainnollisuuden vuoksi tiedot kerätään tässä vaiheessa yhteen taulukkoon. Taulukosta nähdään rekisterin nimi ja käyttötarkoitus, tietojen tallennustapa ja -paikka, rekisterin vastuuhenkilö, pääkäyttäjät ja käyttöoikeudet. Lisäksi taulukosta nähdään rekisterin suojaus, sopimuskumppanit, mitä henkilötietoluokkia / henkilötietoja rekisterissä käsitellään, mikä on rekisterin käsittelyperusta sekä henkilötietojen säilytysaika. Taulukosta ilmenee myös tietovirrat, rekisterin tallennuksen maantieteellinen sijainti sekä tieto keillä muilla toimijoilla on mahdollisuus päästä käsiksi rekisterin tietoihin.

Taulukko 4. Esimerkki henkilörekisterin nykytila-analyysin tuloksesta

Henkilörekisterin nimi / käyttötarkoitus	**Status hautaustoimi**
Tietojen tallennustapa /-paikka	Status ohjelmisto
Tietojen tallennuspaikka	Kirkkohallituksen palvelukeskus
Rekisterin vastuuhenkilö	Toimistonhoitaja
Pääkäyttäjä	Toimistonhoitaja
Käyttöoikeudet	Toimistonhoitaja, talouspäällikkö, hautausmaanhoitaja
Suojaus	Verkon käyttäjätunnus ja salasana Sovelluksen käyttäjätunnus ja salasana
Sopimuskumppanit	Kirkkohallitus, CGI Suomi Oy
Henkilötietoluokat	Arkaluonteiset
Henkilötiedot	Nimi, yhteystiedot, vakaus,
Käsittelyperuste	Hautaustoimen asiakkuus, sopimus omaisen kanssa
Säilytysaika	
Tietovirrat	Paperituloste, siirto Exceliin
Maantieteellinen sijainti	
Muilla mahdollisesti rekisteriin pääsy	Kirkkohallituksen käyttötuki CGI:n sovelluskehitys
Huomioita	Salasana lukkiutuu x virheellisen salasanan jälkeen

Taulukko 5: Rekisterinpitäjän velvollisuudet

Arvion kohde	Kriteerit	Valitse arvo	Lisäselite
Käsittelyperuste on asetuksen	1 Yksiselitteinen suostumus 2 Sopimus 3 Seurakuntalaisen elintärkeä etu 4 Seurakunnan etu 5 Kolmannen osapuolen etu, kenen 0 Ei mikään edellä mainituista	**2**	
Käsittelyperuste on lain mukai	1 Lakisääteinen velvollisuus 2 Yleisen tehtävän hoitaminen 3 Julkisen vallan käyttö 4 Käsittelyperuste asetuksesta 0 Ei mikään edellä mainituista	1	
Käsitelläänkö erityisiä henkilötietoryhmiä Kirjaa käsittelyn perustelut lisäselite kenttään	1 Uskonnollinen vakaumus 2 Terveystieto 3 Seksuaalisuuteen liittyvä tieto 4 Ammattiliiton jäsenyys 9 Ei sisällä arkaluontoista tietoa	**1**	Vainajan tiedot Väestökirjanpidosta
Henkilötietojen kohtuullisuus	1 Kerätään välttämätön tarvittava tieto 2 Tietoa kerätään historian kirjoitusta varten 3 Tietoa kerätään varmuuden vuoksi, voi sitä tarvita	**1**	
Henkilötietojen oikeellisuus Kuvaa lisäselite kentässä miten tietoja ylläpidetään	1 Tiedot ovat ajantasalla 2 Tiedot ovat ajantasalla ja niitä päivitetään säännöllisesti 3 Tiedoissa on puutteita	3	Haudanhaltijat eivät ilmoita muutoksista, joita voi olla mm. haudanhaltijan kuolema, osoitteen tai muun yhteystiedon muuttuminen.
Tietojen säilytysaika Kirjaa peruste säilytysajalle	1 Tarpeen mukainen säilytysaika 2 Tietoa säilytetään varmuuden vuoksi 3 Ei tietoa säilytysajasta	3	Otetaan yhteys Status tukeen.
Tietoturvan ja tietosuojan tasc	1 Turvallisuudesta huolehdittu ohjeiden mukaisesti 3 Epäselvyyttä turvallisuudesta	1	

Taulukossa 5 rekisterin nykytilaa analysoidaan rekisterinpitäjän velvollisuuksien ja rekisteröityjen oikeuksien näkökulmista. Taulukon väreistä voidaan päätellä mihin asioihin seurakunnan tulee kiinnittää erityistä huomiota. Taulukon 5 tuloksen mukaan seurakunnan tulee pohtia miten punaisella oleva tietojen ajantasaisuuden ja oikeellisuuden puute voitaisiin parantaa. Keltainen väri pysäyttää miettimään arkaluonteisten henkilötietojen käsittelyä ja miten tietojen säilytysajat tulee määritellä. Esimerkin mukainen analysointi tehdään jokaiselle henkilörekisterille ja sopimukselle erikseen. Nykytilan kartoituksen ja analysoinnin jälkeen seurakunnalla on karkea kuva tietosuoja-asetuksen haasteista toimintaan.

Seurakunnan tulee arvioida myös seurakuntatasolla tietosuojan kokonaisuuden nykytilanne, ei vain yksittäistä rekisteriä, toimintoa tai sopimusta. Hyvän pohjan tähän arvioon saa JUHTA-VAHTI aineistossa olevalla Tietosuojan tukityökalu Excel-lomakkeesta. Arvioinnin kohteena ovat seurakuntatasolla rekisteröityjen oikeudet, onko seurakunta huomioinut tiedonantovelvollisuuden, onko huolehdittu oikeudesta päästä omiin tietoihin ja mahdollisuus oikaista virheelliset tiedot, onko henkilön oikeus tulla unohdetuksi huomioitu toiminnassa, miten tietojen siirto järjestelmästä toiseen voidaan toteuttaa, miten suhtaudutaan automaattiseen päätöksentekoon ja rekisteröityjen profilointiin sekä miten tietoturvaloukkausten ilmoittamiseen on valmistauduttu.

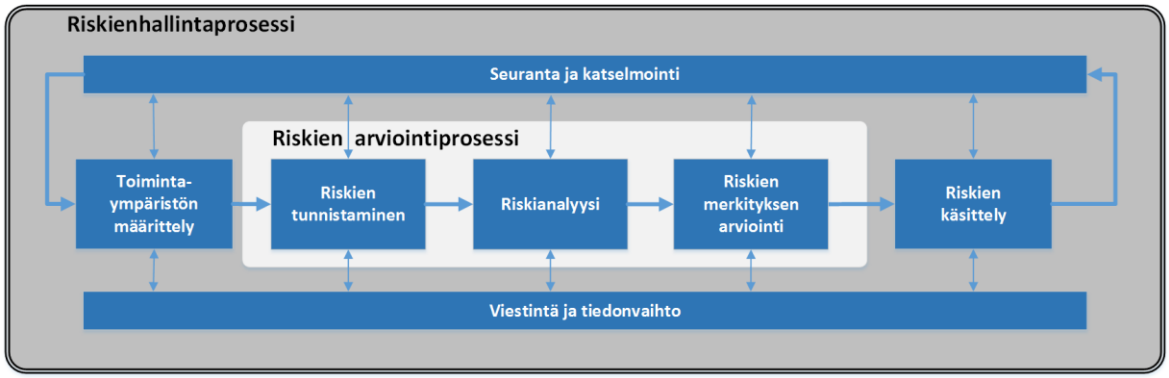
Yllä mainitulla taulukolla voidaan arvioida myös rekisterinpitäjän velvollisuuksien huolehtimisen nykytilasta. Kartoitettavat asiat ovat käsittelyn oikeusperusta, tietosuojavastaavan nimeäminen ja toimenkuva sekä tietosuojaorganisaation toimivuus. Otetaan kantaa onko tietosuojan vuosikello olemassa. Miten riskienhallinta ja vaikutusten arviointi tietosuoja-asioissa toimii. Ymmärretäänkö sisäänrakennetun ja oletusarvoisen tietosuojan ja mikä valmiusaste seurakunnan toiminnassa on näiden osalta. Pohditaan, miten tiedon elinkaaren hallinta on huomioitu sekä mikä merkitys tietosuojalla on hankinnoissa ja projektitoiminnassa (seurakunnassa yleinen projekti on Yhteisvastuukeräys, johon osallistuu suuri joukko vapaaehtoisia). Isona kokonaisuutena on tietoturvallisuuden toteuttamisen arviointi, seurakunnan tulee pohtia mitä toimenpiteitä ja muutoksia tulee tehdä. Pohditaan ja tarkistetaan dokumentaation ja sopimusten tilanne tulevan tietosuoja-asetuksen näkökulmasta.

Kuten keisari Augustukselle sanottiin, johdon on näytettävä esimerkillään ottavansa tietosuoja-asetuksen tosissaan. Nykytilan arviointi ulotetaan myös johdon toimintaan, miten johto on resursoinut hankkeen, millä tavalla koulutus (henkilöstön, luottamushenkilöt ja vapaaehtoiset) on hoidettu ja oppiminen todennettu. Miten tietosuojasta on viestitty ja miten tietosuoja-asetus on huomioitu sekä normaalitilan että poikkeusolojen toiminnassa.

4.4.1 Laadi riskiarvio

Nykytilan kartoituksen ja analysoinnin jälkeen laaditaan riskiarvio kuvan 5 mukaisesti. Riskiarvioinnissa kiinnitetään huomio nykytila-analyysin tuloksena esille tulleisiin riskeihin sekä muihin tunnistettuihin riskeihin. Riskienhallinnassa voi käyttää Kuvan 5 mukaista ISO31000 standardiin perustuvaa prosessia, jonka lähtökohtana on toimintaympäristön määrittely. Sen jälkeen kartoitetaan ja tunnistetaan riskit. Riskien tunnistamisen jälkeen analysoidaan tunnistetut riskit. Analyysin jälkeen arvioidaan riskin merkitys toiminnalle ja

rekisteröidyille henkilöille. Edellä tehtyjen vaiheiden jälkeen määritellään miten riskiä käsitellään, kuka vastaa ja mitä toimenpiteitä tehdään määritellyn ajan puitteissa.



Kuva 5. ISO 31000 standardin mukainen riskienhallintaprosessi. Kuva perustuu standardiin SFS-ISO 31000 (Valtiovarainministeriö 2017).

Toimintaympäristön määrittelyssä kuvataan EU:n tietosuoja-asetuksen asettamat vaatimukset sekä seurakunnan perustiedot. Toimintaympäristön kuvaukseen kuuluu myös dokumentoida riskiarvioinnin suorittaja ja suoritusajankohta sekä muut riskienarviointiin osallistuneet henkilöt. Toimintaympäristössä kuvataan mitä dokumentteja käytetään, minkälaisia dokumentteja ja ohjeita seurakunnalla on käytettävissä. Riskien arvioinnin kohteena voi olla esimerkiksi: Organisaatio, tiedonkäsittelyn prosessi, seurakunnan palvelut, henkilörekisterit, vapaaehtoistoiminta ja yhteistyökumppanit.

Toimintaympäristön kuvaamisen jälkeen määritellään riskiluokat. Riskiluokkana voi olla esimerkiksi: Strateginen riski (seurakunnan tulevaisuus vaarantuu), Toimintaan liittyvä riski (toiminta halvaantuu, vaikeutuu tai estyy), Taloudellinen riski (rahan ja työajan menetys), Vahinkoriski (henkilöstön sairastuminen ylikuormitustilanteessa, rekistereiden tuhoutuminen, laitteiden tuhoutuminen). Määriteltäviin asioihin kuuluu myös riskimatriisin. Riskimatriisissa arvioidaan riskin todennäköisyyttä sekä riskin vaikutusta, näiden lukujen perusteella lasketaan riskin vaikuttavuus. Riskin ja riskin todennäköisyyden arvoina voi olla esimerkiksi: 1 Epätodennäköinen, 2 Mahdollinen, 3 Todennäköinen, 4 Lähes varma. Riskien vaikuttavuuden arvoina voi olla esimerkiksi: 1 Vähäinen / ei vaikutusta. 2 Kohtalainen, 3 Merkittävä, 4 Kriittinen. Käytännössä riskien arviointi tulee tehdä vaiheittain, siten että kutakin riskiä / riskiryhmää ja / tai riskiluokkaa arvioi sellaiset henkilöt jotka tietävät ja tuntevat kyseisen toiminnan. Esimerkiksi diakoniatoiminnan riskienarvioinnissa tulee paikka olla diakoniatyöstä vastaava tai diakonityön hyvin tunteva henkilö.

Taulukossa 6 on selvennetty riskienarvioinnin perustietojen kuvaaminen. Taulukossa on sarake arviointipäiviä varten, arviointiin osallistuneet henkilöt sekä tieto minkälaiset dokumentit ohjasivat riskiarvion tekemistä. Lisäksi kerrotaan mihin riskiluokkaan arvioitava riski kuuluu sekä minkälaisia numeroita arvioinnissa käytetään.

Taulukko 6. Riskiarvioinnin perustiedot

Arvioinnin päivämäärät:	**24.11., 27.11., 30.11.2017**
Arvioinnissa läsnä:	Mxxxx, Yzzzz, Kzxzx
Ohjaava dokumentaatio:	Tietosuoja ja tietoturva Pornaisten seurakunnassa
Riskiluokka:	Toimintaan liittyvä riski
Riskienarvioinnin perustiedot:	Arvioidaan henkilörekistereihin liittyviä riskejä. Nykytila-analyysin perusteella havaittiin olemassa olevissa rekistereissä ongelmia ja haasteita.
Arvioinnin kohteet:	Luottamushenkilörekisterissä on kaikkien seurakunnan luottamustehtävissä toimivien henkilöiden yhteystiedot, mukaan lukien palkkion maksuun liittyvät sekä tieto luottamustehtävistä. Vapaaehtoisetrekisterissä on tieto seurakunnan vapaaehtoisista toimijoista yhteystiedot, mukaan lukien palkkion maksuun liittyvät sekä tieto kiinnostuksen kohteista ja lupauksista toimia vapaaehtoisena. Status hautaustoimen rekisterissä on tiedot Pornaisten seurakunnan hautausmaahan haudatuista sekä haudanhaltijoista.
Kohteen vastuuhenkilö:	Luottamushenkilöt: Kirkkoherra. Hautaustoimi: Talouspäällikkö
Riskin todennäköisyyden arvot:	1 Epätodennäköinen 2 Mahdollinen 3 Todennäköinen 4 Lähes varma
Riskin vaikutuksen arvot:	1 Vähäinen / ei vaikutusta 2 Kohtalainen 3 Merkittävä 4 Kriittinen

Taulukossa 7 on kuvattu varsinainen riskianalyysin tekeminen. Riskit numeroidaan ja riski sekä riskin vaikutus kuvataan. Seuraavaksi arvioidaan riskin todennäköisyys sekä vaikutus, näiden lukujen perusteella lasketaan riskin merkitys (todennäköisyys x vaikutus). Riskin sietokyky arvioidaan edellisten lukujen perusteella, arvioinnissa kannattaa antaa suurempi painoarvo riskin vaikutukselle. Riskin sietokyky arvioidaan asteikolla 0 – 3. Luku 0 tarkoittaa, että riskiä ei voida sietää, seurakunnan on välittömästi määriteltävä toimet riskin poistamiseksi ja / tai minimoimiseksi. Luku 1 tarkoittaa merkittävää riskiä, myös tämän riskin osalta seurakunnan tulee pohtia pikaisia toimenpiteitä riskin poistamiseksi ja / tai minimoimiseksi. Luku 2 tarkoittaa huomioitavaa riskiä, asiaan on puututtava ja toimenpiteet tulee tehdä suunnitelman mukaisesti. Luku 3 tarkoittaa, että riskin kanssa tullaan toimeen,

seurakunta tekee tarpeelliset toimet riskin poistamiseksi ja / tai minimoimiseksi. Riskin sietokyvyn arvo antaa pohjan toimenpidesuunnitelman tehtävien laatimiseksi.

Taulukko 7. Esimerkki riskianalyysin tuloksesta

Toiminnalliset riskit		**Analyysi**				
Riski nro:	**Kuvaus riskistä**	**Toden-näköisyys**	**Vaikutus**	**Riskin merkitys**	**Riskin sietokyky**	**Jatkotoimenpiteet / vastuu**
1	Luottamushenkilöt, Vapaaehtoiset, hautaustoimi: Tietojen ajantasaisuus, muutosten päivittäminen epäonnistuu	4	2	8	2	Yhteydenpidossa luottamushenkilöille, vapaaehtoisille ja hautaustoimen asiakkaille pyydetään päivittämään rekisterissä olevat tiedot. Vuosittain lähetetään viesti aiheesta Vastuu: toimistonhoitaja
2	Tiedot häviävät tietomurron tai ilkivallan takia	2	4	8	0	Otetaan käyttöön henkilöstön tietoturva ja tietosuojakoulutus sekä testit aiheesta. Varmuuskopioinnista huolehtiminen. Yhteydenpito IT-alueen, Kipan ja Kirkkohallituksen kanssa toiminnan varmistamiseksi. Vastuu: Talouspäällikkö
3	Tulostin ei toimi, tuloste jää koneen muistiin ja tulostaa arkaluonteisen asiakirjan ajankohtana, jolloin tieto joutuu ulkopuolisen saataville.	4	3	12	1	On harkittava tietoturvatulostimen käyttöönottoa leasing sopimuksen umpeuduttua. Henkilöstön ohjeistus: Arkaluonteiset tulosteet otetaan omalla koneella. Koneen temppuillessa katkaistaan virrat ja odotetaan uudelleen käynnistystä, tuloste tulee.
4	Kaikilta luottamushenkilöiltä ja vapaaehtoisilta ei ole saatu todennettua lupaa henkilötietojen rekisteröintiä varten. Lähetettyyn lupakyselyyn ei vastata.	4	1	4	3	Voidaan tulkita, että henkilö on antanut suostumuksensa, kun saapuu henkilökohtaisesta kutsusta paikalle. Seurakunnan kotisivuille tehdään ilmoittautumislomake vapaaehtoistoimintaan. Pyydetään lupa sopivassa tilanteessa Vastuu: Kirkkoherra
5	Luottamushenkilöt ja vapaaehtoiset eivät ymmärrä henkilötietojen käsittelyn vaatimuksia. Lörpötellään kylillä nähdystä ja kuullusta esim. ruuanjakajat.	4	3	12	1	Pidetään vapaaehtoisille ja luottamushenkilöille yhteinen tilaisuus, jossa aihe nostetaan esille. Hauskan yhdessä olon puitteissa kerrotaan vakavaa asiaa.

		Riskin sietokykyluokat
		0 = Riskiä on sietämätön
		1 = Merkittävä riski
		2 = Huomioitava riski
		3 = Riskin kanssa tullaan toimeen

4.4.2 Kehittämissuunnitelma

Riskianalyysin tuloksena syntyy priorisoitu lista kehittämiskohteista. Kehittämiskohde avataan ja pohditaan ratkaisujen vaihtoehtoisia toteuttamistapoja. Edellisten vaiheiden aikana (projektisuunnitelma, johdon tahtotila, ohjeistus ja koulutus, nykytila-analyysi ja riskiarvio) listattujen asioiden pohjalta laaditaan kehittämissuunnitelma, jossa määritellään tarvittavat toimenpiteet, aikataulut ja vastuuhenkilöt.

Kehittämissuunnitelmassa kohteet ryhmitellään aihepiirin mukaisiin kokonaisuuksiin. Taulukossa 8 ryhmittelevinä tekijöinä on käytetty toimintatapoja, viestintää, yhteistyötä ja tekniikka. Toimintatavat-otsakkeen alle kootaan kehittämiskohteet, jotka vaikuttavat seurakunnan toimintaan. Tällaisia asioita ovat mm. työntekijöiden, vapaaehtoisten tai luottamushenkilöiden työskentelytapoihin liittyvät asiat. Viestintä-otsakkeen alle kootaan koulutukseen ja viestintään liittyvät kehittämisaiheet. Yhteistyö-otsakkeen alle tulee kaikkia sopimustoimintaan liittyvät kehittämiskohteet. Tekniikka-otsakkeen alle kirjataan aiheet, jotka koskettavat tieto- tai muuta tekniikkaa. Kehittämiskohteelle määritellään vastuuhenkilö, aikataulu sekä tieto mihin riskianalyysin kohtaan kehittämisehdotus liittyy.

Taulukko 8: Kehittämissuunnitelman malli

Tehtävä / vko	Vastuu	45	46	50	51	52	3	6	7	11	12	13	19	20	21	Tehtävän tarkennus	Riski
Toimintatavat																	
Vapaaehtoisten suostumusten hallinta	KH															Pyydetään vapaaehtoisia antamaan todennettavan suostumuksen. Seurataan ilmoittautumisia, aktivoidaan ihmisiä antamaan suostumus. Luodaan erilaisia menettelytapoja	4
Vapaaehtoisten koulutus	KH															Annetaan vapaaehtoisille koulutusta henkilötietojen käsittelystä. Vapaaehtoiset käsittelevät henkilötietoja esim. leivänjaon yhteydessä.	5
Monitoimikoneen käytön ohjeistus	TP															Monitoimikoneen läheisyyteen laitetaan ohjeistus koneen uudelleen käynnistämiseksi ja / tai työn poistamiseksi tulostusjonosta.	3
Vapaaehtoisrekisterin yhtenäistäminen	KH															Luodaan yksi keskitetty vapaaehtoisrekisteri, jossa on "täppä" kiinnostuksen kohteista. Tavoitteena helpottaa ylläpitoa.	
Viestintä	KH																
Tiedottaminen seurakuntalaisille	KH															Kirjoitetaan aiheesta kuukausitiedotteessa, lähetään postia ja / tai sähköpostia vapaaehtoisille, pyydetään suostumuksia.	4
Työntekijäkokoukset	TP															Tilannekatsaus esillä työntekijäkokoukissa	
Kirkkoneuvoston kokoukset	TP															Kirkkoneuvoston kokouksissa annetaan tilannekatsaus, samalla kerrotaan tietosuoja-asetuksen vaikutuksesta luottamushenkilöiden toimintaan	5
Yhteistyö muiden toimijoiden kanssa																	2
KustensIT käytännöt/ sopimukset	TP															Käydään läpi varmistukset, tietoturva ja sopimukset	2
KIPA käytännöt/ sopimukset	TP															Käydään läpi varmistukset, tietoturva ja sopimukset	2
Status käytännöt/ sopimukset	TP															Käydään läpi varmistukset, tietoturva ja sopimukset	2
Katrina käytännöt/ sopimukset	TP															Käydään läpi varmistukset, tietoturva ja sopimukset	2
Tietosuojavastaavan nimitys	KH																
Tekniikka																	
Tietoturvatulostimen hankinta	TP															Huomioidaan leasing-sopimuksen päättymisen jälkeen	3
Nettisivuille ilmoittautumislomake.	KH															Laaditaan lomake, jossa pyydetään tekijän suostumus . Kirkkoväärtien ilmoittautumislomake ok	4

4.5 Seuranta ja raportointi

Seurannan ja raportoinnin yksi tehtävä on varmistaa, että projekti- ja kehittämissuunnitelmassa määritellyt tehtävät tulevat hoidettua ajallaan. Seurakunnan kannattaa heti hankkeen alkuvaiheessa tehdä päiväkirja, johon kirjataan kaikki hankkeen keskeiset tehtävät. Seuranta ja raportointi varmistavat sen, että myös luottamushenkilöjohto on tietoinen EU:n tietosuoja-asetuksen mukanaan tuomista vaatimuksista seurakunnan toimintaan. Toinen tehtävä tulee EU:n tietosuoja-asetuksen vaatimasta osoitusvelvollisuudesta. Säännöllinen raportointi kirkkoneuvostolle kertoo sen, että seurakunta on ottanut tietosuoja-asetuksen velvoitteet vakavasti. Vuosittainen tietotilinpäätös on luontevinta sisällyttää seurakunnan

tilinpäätökseen ja toimintakertomukseen (Tasekirja). Mallipohjan seurakuntien tasekirjan pohjan luo Kirkkohallitus, olen ollut yhteydessä pohjan luojaan ja pyytänyt lisäämään kohdan tietosuoja-asetuksen raportointivelvollisuuden täyttämiseksi.

4.6 Tiivistelmä tarvittavista toimenpiteistä

EU:n tietosuoja-asetuksen vaatimien tehtävien tekeminen tulee aloittaa välittömästi, sillä asetus astuu voimaan 25.5.2018. Osoitusvelvollisuuden täyttämiseksi on ensimmäisenä tehtävänä hyvä tehdä päiväkirja, johon merkitään kaikki tietosuoja-asetuksen käyttöönottoon liittyvät tehtävät. Pienissä seurakunnissa kannattaa käyttää hyväksi olemassa olevia tietosuoja- ja tietoturvapolitiikka määritelmiä. Tietoturvamääräyksissä kannattaa viitata kirkkohallituksen antamiin ohjeisiin, jotka on syytä lukea viimeistään tässä vaiheessa.

Henkilöstön koulutus ja koulutuksen todentaminen on mielestäni helpointa hoitaa arjentietosuoja.fi aineiston avulla. Tämän jälkeen kannattaa kartoittaa olemassa olevat henkilötietorekisterit. Arvioi sopimusten kartoituksen aluksi sisältääkö sopimus henkilötietojen käsittelyä. Nykytila-analyysissa verrataan nykytilaa tietosuoja-asetuksen ja tietoturvan perusperiaatteisiin (lainmukaisuus, kohtuullisuus, läpinäkyvyys, käyttötarkoituksenmukaisuus, täsmällisyys, minimointi, säilytysaika). Tämän jälkeen arvioidaan henkilötietojen käsittelyyn liittyvät riskit ja laaditaan kehittämissuunnitelma. Kehittämissuunnitelmassa on syytä priorisoida asiat ainakin kustannusten, toteutusmahdollisuuksien sekä käytettävissä olevan ajan ja resurssien perusteella.

Kokemukseni mukaan järkevin tapa toteuttaa hanke on tehdä se pienissä palasissa, ja ratkaistaan ongelmat heti kun pystytään. Isot asiat pohditaan ja priorisoidaan erikseen. Tietosuoja-asetuksen käyttöönotossa tulee eteen paljon pieniä, nopeasti ratkaistavia asioita. Pieni, mutta merkityksellinen asia on muistutus tietokoneen lukitsemisesta tai henkilötietoja sisältävien papereiden siirtäminen lukkojen taakse.

Seuraavassa on luettelo tärkeimmistä toimenpiteistä:

1. Luo päiväkirja tietosuoja-asetuksen toimenpiteiden seurantaa varten.
2. Kirjoita tietosuoja-ja tietoturvapolitiikat ja määräykset, kuvaa käsittelytoimet.
3. Tee projektisuunnitelma.
4. Viesti asiasta henkilöstölle ja luottamushenkilöille, seuraa projektin etenemistä.
5. Vaadi henkilöstöä katsomaan arjentietosuoja.fi video.
6. Vaadi tekemään tietosuojatesti. Valvo suorituksia.
7. Kartoita olemassa olevat henkilörekisterit ja sopimukset.

8. Tekee nykytila-analyysi.
9. Tee riskianalyysi.
10. Tee kehittämissuunnitelma, toteuta suunnitelma.
11. Ota yhteys järjestelmätoimittajiin ja yhteistyökumppaneihin, päivitä sopimukset.
12. Kirjoita tietosuojaselosteet ja henkilötietojen käsittelyohjeet. Tee prosessikaaviot rekisteröityjen oikeuksista. Laadi tietosuojatyön tiekartta.
13. Seuraa tietosuojan tilannetta jatkuvasti. Tee tietotilinpäätös.

Seurakunnissa on vuosituhannet käsitelty arkaluonteisia tietoja, perinteet ovat pitkät. Tietotekniikan yleistyminen, vapaaehtoisten lisääntyvä mukana olo ja sosiaalinen media ovat kuitenkin luoneet uusia toimintatapoja. Uusia toimintatapoja ei ole aina arvioitu tietosuojan ja -turvan näkökulmista.

Ylläoleva tietosuojan käyttöönotto projekti on itseasiassa prosessi, samat asiat toistuvat vuodesta toiseen. Vuosittain seurataan tietosuoja-asioita, kouluttaudutaan, analysoidaan, arvioidaan riskit, toteutetaan tarvittavat toimenpiteet ja tehdään tietotilinpäätös.

Parastapa valloittaa maailma on ottaa ensimmäinen askel ja sen perään toinen. Parastapa toteuttaa tietosuoja-asetuksen vaatimukset on aloittaa työ heti ja edetä pienin, mutta ripein askelin kohti 25.5.2018 tapahtuvaa tietosuoja-asetuksen voimaantuloa.

5 Pohdinta

Tämän opinnäytetyön tavoitteena on ollut luoda työohje tietosuoja-asetuksen käyttöönottamiseksi seurakunnassa. Kappaleessa 4.6 olen tiivistänyt asetuksen käyttöönottoon ja toiminnan ylläpitämiseen liittyvät tehtävät. Opinnäytetyössäni olen pohtinut tietosuoja-asetuksen vaikutusta toimintaan ja henkilörekistereihin. Työn aikana olen havahtunut huomaamaan, että poistuessani työhuoneesta tietokone on jäänyt lukitsematta ja pöydällä on saattanut olla henkilötietoja sisältävä asiakirja. Olen opetellut ja ainakin osittain oppinut lukitsemaan tietokoneen ja arkistoimaan asiakirjat välittömästi. Tietosuojaroskis on tullut tutuksi.

On ollut hämmentävää todeta, etten tiennyt olemassa olevista henkilörekistereistä. Yhtä hämmentävää on ollut huomata, ettemme tienneet missä kaikissa toiminnoissa vapaaehtoiset ovat mukana. Nyt tiedän! Ainakin osittain. Yhteisissä työkokouksissa sekä kirkkoneuvoston kokouksissa olemme pohtineet tietosuoja-asetuksen vaikutusta toimintaan. Keskustelut ovat avanneet näkökulman toiminnallisen puolen haasteisiin. Olemme löytäneet yhteisen tahtotilan ratkaista eteen tulevia haasteita. Yhteinen henkilörekisteri ei olekaan mörkö, vaatimusmäärittelyt on aloitettu. Keskusteluissa on esitetty monia kysymyksiä. Olen opetellut pohtimaan asiaa kysyjän näkökulmasta, osittain koen onnistuneeni tässä asiassa.

Kun aikanaan olin pikaisesti tutustunut EU:n tietosuoja-asetukseen, se vaikutti kohtuullisen helppotajuiselta ja ymmärrettävältä. Tarkempi paneutuminen asiaan auttoi ymmärtämään kuinka vähän olin ymmärtänyt. Mukailen aikanaan kokemaani ”ahaa-elämystä”: Nuorena tiesin paljon enemmän kuin nyt, vaikka tässä välissä olen oppinut vaikka kuinka paljon. Näin taitaa käydä asiassa kuin asiassa. Paneutumalla asiaan huomaan kuinka monia eri näkökulmia kätkeytyy tähänkin asetukseen.

Opinnäytetyön kirjoittamisen aikana vietimme 100 vuotiaan Suomen itsenäisyyspäiväjuhlia. Olen havahtunut huomaamaan, että seurakunnaltamme puuttuu projektityömenetelmät ja ohjeet. Kuitenkin teemme jatkuvasti eri suuruusluokkaa olevia projekteja, esimerkkinä olkoot Yhteisvastuukeräys. Opin työn kirjoituksen aikana, että yksi seuraavista ponnisteluiden kohteista on tuoda seurakuntaan projektityön menetelmiä ja osaamista.

Aikaisemmin työskentelin pitkään toiminnankehittämisen konsulttina. Kokemukseni mukaan nykytilan analysointi nähdään usein turhaksi ja aikaa vieväksi toiminnaksi. Niin nytkin. Monen mielestä tärkeintä on päästä päämäärään. Yleinen ajatus on; ”Taas turhaa hallinnon byrokraattisia tehtäviä, asia ei kosketa minua”. Samoin saatetaan ajatella, että

seurakunnilla on samat tietojärjestelmät, eli riittää kun yksi tekee ja muut seuraavat ja kopioivat tuloksen. Ajatus pitää osittain paikkaansa, tietojärjestelmien osalta, mutta jokaisessa seurakunnassa on omat toimintatavat. Havaitsin, että on tärkeää kertoa mitä tietosuoja-asetus voi oikeasti tarkoittaa. Se ei ole uhka vaan mahdollisuus järkeistää toimintaa. Opin perusteluiden tärkeyden. Opin että on hyvä pohtia ratkaisuvaihtoehtoja kiihkottomasti ja arvioida ratkaisujen vaikutuksia toimintaan ja teknologiaan.

Johdon suhtautuminen tietosuojaan luo perustan organisaation turvallisuuskulttuurille. Tietosuoja-asetuksen merkityksen vähättely luo ”hälläväliä” kulttuurin, työmäärän voivottelu latistaa ja masentaa sekä antaa mahdollisuuden vetäytyä ”oikeiden töiden” taakse. Asiallinen, ”kääritään hihat ja aletaan töihin”, asenne antaa esimerkin, että olemme tosissamme. Kiitos Kari, että suoritit välittömästi tietosuojatestin. Opin sisäistämään johdon sitoutumisen merkityksen.

Työtä hankaloitti se, että EU:n tietosuoja-asetuksen soveltamista on tehty vielä kohtuullisen vähän kirkossa. Työn edetessä aineistoa alkoi löytymään kaupallisten toimijoiden tekemänä (tietojärjestelmätoimittajat ja eläkeyhtiöt). Koin, että paras ja luotettavin lähde oli Valtiovarainministeriön ja Kuntaliiton yhteishanke. Osallistuin Vahti-työpajaan opinnäytetyön kirjoittamisen aikana. Työn aikana selvisi, että eräs entinen seurakunnan luottamushenkilö toimii erään kunnan tietosuojavastaavana. Verkostoitumisen jalo taito kirkastui.

Seurakuntien toimintaa ohjaavat osaltaan Kirkkohallituksen antamat ohjeet ja määräykset. Kirkkohallituksen tietosuojavastaava ohjeistaa seurakuntien toimintaa, näitä ohjeita ja määräyksiä kannattaa seurata. Ohjeet löytyvät kirkon Nuotta-intrasta. Tällä hetkellä pohjadokumentteja ei ole, ja ohjeistuksen määrä on vähäinen. Koska seurakunnat eivät kilpaile jäsenistä toistensa kanssa, niiden kannattaa tehdä yhteistyötä sekä tietosuoja-asetuksen käyttöönottovaiheessa että tietosuojan seuraamisessa. Käytännön yhteistyö tuntuu kuitenkin olevan useissa tapauksissa vaikeaa. Olisi luonnollista, että Kirkkohallitus luo pohjadokumentit joita seurakunnat, seurakuntayhtymät ja it-alueet voisivat hyödyntää. Yhteisiä pohjadokumentteja puoltaa se, että kirkolla on käytössä yhteisiä järjestelmiä sekä yhteiset normit ja ohjeet. Monessa asiassa seurakunnalla ei ole valinnanvaraa, Kirkkohallitus ja tuomiokapituli määrää suunnan ja tahdin. Opin yhteistyön tekemisen haasteellisuuden, aikaisemmin oppimani asia syventyi. Konsulttina oli helpompi ohjeistaa yhteistyöhön, kun käytännön tekijänä toteuttaa yhteishanke.

Usein muutosta vähätellään tai ylidramatisoidaan. Muutokseen liittyy aina pelkoja ja vastustusta. Yleensä pelot liittyvät oman osaamisen riittävyyteen, toisaalta totutusta toimintatavasta luopumisen tuskaan, kolmanneksi oman vallan tai hallinnan kapenemisen pelosta.

Tässä kehittämishankkeessa osaamisenpelko näkyy tietoturvatestin kartteluna, syyksi kerrotaan ”ei ole aikaa”. Omasta tutusta turvallisesta toimintatavasta luopumisen pelko näkyy kommentista ”Tarkoitatko oikeasti sitä, että minun pitäisi kysyä kaikilta niiltä jotka vuosikymmenten aikana ovat olleet mukana xxx-toiminnassa suostumus?”. Vallasta luopumisen pelko näkyy kommentissa ”Mutta tämähän tarkoittaa sitä, että meidän vapaaehtoisia houkutellaan muihin tehtäviin ja se taas tarkoittaa sitä, että minun pitää hankkia uusia vapaaehtoisia. Mistä luulet, että heitä saa? Ja luuletko, että niitä saa helpolla?”. Pelot kannattaa tunnistaa ja tunnustaa heti hankkeen alussa. Kokemukseni mukaan peili on hyvä, usein jopa paras konsultti. Kysymällä itseltäni ja vastaamalla rehellisesti kysymyksiin: mikä pelottaa, miksi pelottaa, mitä voi pahimmillaan tapahtua, löydän keskeisiä pelon syitä. Pelot liittyvät siis itseeni, ei niinkään organisaatioon eli seurakuntaan.

Opin ymmärtämään omia pelkojani: Entä jos en ymmärrä ja osaamattomuuteni paljastuu? Taas ylimääräistä työtä, juuri kun olen saanut tilanteen haltuun? Yhteistyö ei kuitenkaan toimi. Kokemukseni syventyi, kahvipöytä- ja käytäväkeskustelut ovat hyvä keino pelkojen poistamiseen. Näissä keskusteluissa ihmiset avautuvat kohtuullisen helposti. Kokemukseni mukaan ongelmaa ei kannata heti ratkaista toisen puolesta, vaan auttaa henkilöä löytämään itse niihin ratkaisuja.

Opin paremmin ymmärtämään kuuntelemisen jalon taidon merkityksen muutoshankkeissa. On helpompi sitoutua asiaan, jonka olen itse keksinyt, kuin asiaan joka on pakko tehdä. Oivallukseni ihmisen käyttäytymisestä kirkastui, sitoutuminen on sisäistä paloa tai ainakin vankkaa velvollisuuden tunnetta. Tunnistamalla ja tunnustamalla vastarinnan, pystyy valitsemaan oikeat ja tehokkaat keinot niiden voittamiseksi. Toivon, että mieleeni jää itämään ja kasvamaan ajatus ”Kuvaa muutoksen merkitys, vaihtoehdot ja seuraamukset. Auta ihmistä löytämään ratkaisu”.

Käytännössä käytettävästä kalenteriajasta johtuen, tietosuoja-asetuksen käyttöönoton ideana tulisi olla Scrum-tyyppinen vaiheittainen lähestymistapa. Tässä toteutustavassa asioita toteutetaan nopeasti vaiheittain, tartutaan pikaisesti niihin asioihin joiden hoitaminen tuntuu luonnolliselta ja helpolta. Suunnittelun lähtökohtana on kuitenkin projektisuunnitelmassa määritelty aikatauluraami. Toteutettava aihekokonaisuus suunnitellaan, tehtäville määrätään vastuuhenkilö ja aikataulut. Toteutuksen vaarana on, että asiat otetaan liian kevyesti ja asiat hoidetaan vasemmalla kädellä. Vaiheittainen toteuttaminen voi tarkoittaa sitä, että asioihin joudutaan palaamaan ja korjaamaan tehtyjä valintoja. Tämä taas nostaa helposti tunteita pintaan, kommentti ”eikö näitä asioita voida hoitaa kerralla kuntoon” voi tulla tutuksi. Vaihtoehtoinen lähestymistapa olisi perinteinen vesiputousmalli, jossa asiat suunnitellaan huolella ja tehdään järjestyksessä. Projektisuunnitelman mukaan

(kohta 4.1.) toteutettavia kokonaisuuksia ovat: 1) Johdon tahtotilan määrittely, 2) Ohjeistus ja koulutus, 3) Analyysit ja kehittäminen sekä 4) Seuranta ja raportointi. Toivon, että olen oppinut perustelemaan asioita ymmärrettävästi.

Tavoitteena on, että 25.5.2018 Pornaisten seurakunnan toiminta vastaa EU:n tietosuoja-asetuksen määräyksiä. Johdon sitoutuminen asioiden edistämiseen ja mahdollisiin ongelmakohtiin puuttuminen on ratkaisevan tärkeää. Tietosuojavastaavan nimeämisessä odotamme hiippakunnan ja it-alueen ratkaisuja. Itse tulen toimimaan tietosuojan yhteyshenkilönä, tietosuojavastuut tulee vielä nimetä. Olemme tunnistaneet henkilötietoja käsittelevät yksiköt, henkilötietojen omistajuuden määrittely on vielä alkutekijöissään. Aiheen äärellä voivat tunteet leiskahtaa. Toivottavasti olen oppinut kuuntelemaan kärsivällisesti ja tuomaan rakentavan ehdotuksen työkuorman alla puurtavalle lähimmäiselleni, työkaverilleni.

Tämä kehittämishanke on alkumetreillään. Toimeen on tartuttu, paljon on tehty, mutta paljon on vielä tekemättä. Olemme laatineet tietosuoja- ja tietoturvapolitiikan, tarkentaneet tietoturvamääräyksiä. Henkilöstölle on kerrottu aiheesta, koulutusvideon katsomiseen on kannustettu ja testin tekemistä rohkaistu. Olemme soveltaneet vapaasti Scrum:n toimintatapaa, ottaneet pienen otannan ja pohtineet mitä tämä tarkoittaa. Kirkkoväärtirekisterin kartoituksen jälkeen totesimme, että jatkossa meillä tulee olla vain yksi vapaaehtoisten ja luottamushenkilöiden rekisteri, muuten tietojen oikeellisuus-vaatimusta ei voida täyttää. Tämän jälkeen heräsi kysymys, mihin järjestelmään perustamme rekisterin. Katrina on käytössä, mutta se tuntuu kömpelöltä. Excel toisi joustavuutta, mutta miten seurannan vaatimus toteutetaan. Pohdinta on kesken, mutta tämän vaiheen (sprintin) jälkeen tiedämme, että vapaaehtoisten tehtävät tulee listata ja saattaa erilaiset tehtävät kaikkien tietoisuuteen. Selkeää tietoa vapaaehtoisten työstä ei olekaan. Tietoa on paljon, mutta se on hajallaan. Jatkotutkimisen arvoinen asia on vapaaehtoisten ja luottamushenkilöiden yhteisen henkilörekisteriohjelmiston tarve seurakunnissa ja järjestöissä.

Virallisia EU-tietosuoja-asetuksen dokumentteja lukiessa jää avoimia kysymyksiä, mistään ei tunnu löytyvän henkilötietoryhmän määritelmää. Avoimeen kysymykseen olen pyytänyt vastausta Tietosuojavaltuutetun toimistosta, Valtiovarainministeriöstä ja Kuntaliitosta. Minulla on arvaus mitä termillä tarkoitetaan, mutta haluaisin asiaan perehtyneiltä tahoilta vastauksen. Odotellaan toinenkin kuukausi, uskon että jossain vaiheessa saan vastauksen. Olen oppinut sietämään epävarmuutta ja keskeneräisyyttä sekä itsessäni että toisissa.

Tein tätä työtä toimintasuunnitelman ja talousarvion laadinnan lomassa. Seurakunnassa joulu on kiireistä aikaa, varsinaisentoiminnan henkilöt haluavat luonnollisesti keskittyä

heille tärkeiden tehtävien suunnitteluun ja hoitamiseen. Pienen organisaation etuna on, että voin astua rinnalle ja auttaa kartoitusten tekemisessä. Jälleen kerran palautuu mieleen, että muutoksessa vaikeinta on vanhasta poisoppiminen. Toinen haasteellinen asia on keskittyä olennaiseen ja saada toiminnan ihmiset innostumaan monen mielestä turhasta asiasta. Asenne ratkaisee, kuten Suomen 100-vuotisjuhlaa viettäessä olemme kuulleet. Ylivoimaisen haasteen edessä tarvitaan yhdessä tekemistä, sitoutumista ja toimeen tarttumista. Keskeinen oppini kiteytyy ajatukseen ”Asetun toisen asemaan. Pohdi miten itse ihan oikeasti toimisin, kun työtä on yllin kyllin ja edessä käsittämätön EU:n vaatimus. Mietin sen jälkeen, miten voitan itsestäni kumpuavan vastarinnan”. Rehellisyys oman vastahakoisuuden edessä auttaa löytämään keinoja, loppu on ihmisten tekemää työtä. Minua on mahdoton sitouttaa, mutta sitoutumistani voi helpottaa löytämällä tekemiselle merkityksen. Motivaatio ja sitoutuminen kumpuavat sisältä.

Mielestäni jatkotutkimuksen arvoinen asia on tutkia miten seurakunnan vapaaehtoisten koulutus ja sitouttaminen tietosuoja-asetuksen vaatimuksiin olisi parasta tehdä. Vapaaehtoisia toimii seurakunnassa monissa eri tehtävissä ja he käsittelevät usein henkilötietoja. Esimerkiksi rippikoulun Innostaja (isonen) käsittelee sekä uskonnolliseen vakaumukseen että terveyteen liittyviä tietoja. Luulisin, että asiaan on havahduttu jo henkilötietolain voimassa ollessa.

Toinen jatkotutkimuksen arvoinen asia on seurakunnan keskitetyn henkilörekisterin määrittely. Miten voisimme hyödyntää kaikkia käytettävissä olevia kanavia tavoittaa ihmisiä ja tarjota heille mahdollisuutta kokea kuuluvansa seurakuntayhteisöön. Rekisterin avulla tulisi voida lähestyä henkilökohtaisesti niitä ihmisiä, jotka ovat ilmaisseet kiinnostuksensa johonkin seurakunnan toimintamuotoon. Olkoon toiminta sitten hautausmaan haravointia, kävelyretkelle osallistumista tai messussa avustajana toimiminen. Kanavia tavoittaa ihmisiä on nykyään paljon, olisi hienoa, että pystyisin kertomaan mikä on minulle mieluisin tapa saada tietoa tulevista tapahtumista tai muusta mielenkiintoani herättävistä asioista.

Kolmas jatkotutkimuksen arvoinen asia on tietosuoja-asetuksen käyttöönotto yhdistyksissä ja järjestöissä. Isot, ammattimaisesti johdetut järjestöt, huolehtivat varmasti asiasta, mutta miten pienet vapaaehtoisvoimin toimivat yhdistykset toimivat. Asia on tärkeä, koska monissa yhdistyksissä käsitellään arkaluonteista tietoa, kuten terveyteen tai vakaumukseen liittyvää tietoa. Tällaisia järjestöjä ovat mm. terveys-/sairausyhdistykset (syöpäyhdistys, mielenterveyden kuntoutujat, paikalliset poliittiset järjestöt, partio).

Neljäntenä mielenkiintoisena tutkimushankkeena on tietosuoja-asetuksen vaikutus seurakunnan / organisaation johtamisjärjestelmiin.

Lähteet

EUROOPAN UNIONIN PERUSOIKEUSKIRJA 2012/C 326/02. Luettavissa: http://eur-lex.europa.eu/legal-content/FI/TXT/?uri=CELEX%3A12012P%2FTXT. Luettu: 29.9.2017

Euroopan Unionin sisäasioiden rahastot. Luettavissa: http://eusa-rahastot.fi/etusivu. Luettu: 15.10.2017

Grimberg C. 1930. Kansojen historia, neljäs osa. Luettu: 18.10.2017

Laki tietosuojalautakunnasta ja tietosuojavaltuutetusta 30.4.1987 1987/474. Luettavissa: http://www.finlex.fi/fi/laki/alkup/1987/19870474. Luettu: 1.10.2017

Haaga-Helia 2013. Tutkintosääntö. Luettavissa: http://www.haaga-helia.fi/fi/opinto-opas/yleista-hhsta/tutkintosaanto. Luettu: 25.9.2017.

Haaga-Helia Vastuullista liiketoimintaa tukevat johtamisjärjestelmät. Luettavissa: myy.haaga-helia.fi/~jokta/aaakeke/kekehallintaymparisto.ppt. Luettu: 18.10.2017

Helsingin Yliopisto, opiskelijan digitaidot. Luettavissa: http://blogs.helsinki.fi/opiskelijan-digitaidot/4-tietoturva/4-1-tietoturvan-ja-tietosuojan-perusteet/tietoturvan-edellytykset. Luettu: 17.10.2017

Inspecta. Luettavissa: https://www.inspecta.fi/Palvelut/Sertifiointi-ja-arviointi/Johtamisjarjestelmasertifiointi/tietoturvallisuus/Tietoturvallisuuden-johtamisjarjestelman-sertifiointi-ISO-IEC-27001. Luettu: 29.9.2017

Kirkkohallituksen yleiskirje 2017. Luettavissa: http://sakasti.evl.fi/sakasti.nsf/0/5DEC06923D5C9F94C22580B1004A8EAF/$FILE/2017-6.pdf. Luettu: 29.9.2017

Kirkkohallituksen päätös kirkon tietoturvamääräyksistä, MEIDÄN KIRKON TIETOTURVA-POLITIIKKA 2012, KIRKON YLEISET TIETOTURVAMÄÄRÄYKSET 2016, Salassapitosopimus. Luettu: 1.11.2017

Kirkkohallitus 2016. Kirkon yleiset tietoturvamääräykset 2016. Luettu: 1.11.2017

Laakso M. 2010. PK-yrityksen tietoturvasuunnitelman laatiminen. Luettavissa: http://www.theseus.fi/bitstream/handle/10024/20793/laakso_matti.pdf?sequence=1&isAllowed=y. Luettu: 29.9.2017

Lääkäriliitto. https://www.laakariliitto.fi/liitto/etiikka/hippokrateen-vala. Luettu: 18.10.2017

OpiTietosuojaa.fi. Luettavissa: https://opitietosuojaa.fi/index.php/fi/aloitus/tietosuoja. Luettu: 1.10.2017

Oikeusministeriö 2017: Miten valmistautua EU:n tietosuoja-asetukseen. Luettavissa: http://www.tietosuoja.fi/material/attachments/tietosuojavaltuutettu/tietosuojavaltuutetuntoimisto/oppaat/1Em8rT7IF/Miten_valmistautua_EUn_tietosuoja-asetukseen.pdf. Luettu: 15.10.2017

Tietosuoja-asetus 679/2016/EU.

Euroopan parlamentin ja neuvoston asetus luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta (EU) 2016/679. Annettu 27.4.2016.

Luettavissa: http://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=CELEX:32016R0679&qid=1512753727149&from=FI. Luettu: 30.9.2017

Tietosuojadirektiivi 680/2016/EU.

Euroopan parlamentin ja neuvoston direktiivi luonnollisten henkilöiden suojelusta toimivaltaisten viranomaisten suorittamassa henkilötietojen käsittelyssä rikosten ennalta estämistä, tutkimista, paljastamista tai rikoksiin liittyviä syytetoimia tai rikosoikeudellisten seuraamusten täytäntöönpanoa varten sekä näiden tietojen vapaasta liikkuvuudesta (EU) 2016/680, 27.42016. Annettu 27.4.2016.

Luettavissa: http://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=CELEX:32016L0680&from=FI. Luettu: 29.9.2017

Valtiovarainministeriö 2003. Ohje riskien arvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa. Luettavissa: https://www.vahtiohje.fi/c/document_library/get_file?uuid=d1bcc4b1-789e-4ce1-a44a-e591a60985b5&groupId=10229. Luettu: 20.10.2017

Valtiovarainministeriö 2004. Ohje riskien arvioinnista Tietoturvallisuuden edistämiseksi Valtionhallinnossa 7/2003. Luettavissa: https://www.vahtiohje.fi/c/document_library/get_file?uuid=d1bcc4b1-789e-4ce1-a44a-e591a60985b5&groupId=10229. Luettu: 29.9.2017

Valtiovarainministeriö 2016a. Toiminnan jatkuvuuden hallinta. Luettavissa: https://www.vahtiohje.fi/c/document_library/get_file?uuid=11459f91-91c8-4ebe-a34f-9d8d9bfc964c&groupId=10229. Luettu: 21.10.2017

Valtiovarainministeriö 2016b. EU-tietosuojan kokonaisuudistus. Luettavissa: https://www.vahtiohje.fi/c/document_library/get_file?uuid=ddb05959-40d1-435f-af23-fd20fc21d63f&groupId=10229. Luettu: 26.10.2017

Valtiovarainministeriö 2017. VM 22/2017 Ohje riskienhallintaan. Luettavissa: https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/80013/Liitteet_VM22_2017.pdf?sequence=2. Luettu: 2.11.2017

Valtiovarainministeriö. Arjentietosuoja.fi. Luettavissa: http://tietosuoja.vahtiohje.fi/fi/#/front. Luettu: 21.10.2017

Valtiovarainministeriön JUHTA-VAHTI-yhteishankkeissa julkaistuja työkaluja. Luettavissa: http://vm.fi/juhta-vahti-yhteishankkeiden-materiaalit. Luettu: 2.10.2017

Valtiovarainministeriö. VAHTI-materiaalit ja –tilaisuudet, 22/2017. Luettavissa: http://vm.fi/vahti-materiaalit-ja-tilaisuudet. Luettu: 2.11.2017

VirtuaaliAMK, Liiketoiminnan kehittäminen. Luettavissa: http://elearn.ncp.fi/materiaali/uimonenj/VirtAMK/tturva.html. Luettu: 28.9.2017

Liitteet

Liite 1. Tietosuoja ja tietoturva Pornaisten seurakunnassa

TIETOSUOJA JA TIETOTURVA

Saarnio Rauno
Opinnäytetyö

TIETOSUOJA-ASETUS

EU:n tietosuoja-asetus GDPR

TIETOSUOJA JA TIETOTURVA PORNAISTEN SEURAKUNNASSA

Dokumentti sisältää Pornaisten seurakunnan tietosuojan ja tietoturvan ohjaavan dokumentaation, kuten tietosuoja- ja tietoturvapolitiikat sekä niihin liittyvät määräykset

1. Tietosuojapolitiikka

Pornaisten seurakunta noudattaa EU:n tietosuoja-asetuksen ja kansallisen lainsäädännön asettamia velvollisuuksia rekisterinpitäjän velvollisuuksista. Kaikessa toiminnassa otetaan huomioon rekisteröityjen oikeudet.

Tietosuojasta vastaa talouspäällikkö yhdessä kirkkoherran ja kirkkoneuvoston kanssa. Talouspäällikkö toimii tietosuoja-asioissa asiantuntijana ja yhteyshenkilönä.

2. Tietoturvapolitiikka ja tietoturvamääräykset

Pornaisten seurakunta noudattaa Kirkkohallituksen ja kirkolliskokouksen määräyksiä ja ohjeistuksia.

Ohjaavia dokumentteja vuonna 2017 ovat:

Kirkkohallituksen päätös Nro 120 kirkon tietoturvamääräyksistä
MEIDÄN KIRKON TIETOTURVAPOLITIIKKA 2012
KIRKON YLEISET TIETOTURVAMÄÄRÄYKSET 2016
Salassapitosopimus

3. Seloste käsittelytoimista

Rekisterinpitäjä:	Pornaisten seurakunta
Sähköposti:	pornaisten.seurakunta@evl.fi
Puhelin:	019 529 6600
Osoite:	Kirkkopolku 4, 07170 Pornainen
Rekisterinpitäjän edustaja:	Talouspäällikkö
Sähköposti:	pornaisten.seurakunta@evl.fi
Puhelin:	040 – 0192 5225
Osoite:	Kirkkopolku 4, 07170 Pornainen
Tietosuojavastaava:	xxxx
Sähköposti:	pornaisten.seurakunta@evl.fi
Puhelin:	040 – 0192 5225
Osoite:	Kirkkopolku 4, 07170 Pornainen

Henkilörekisteriä pidetään Pornaisten seurakunnan toiminnan mahdollistamiseksi. Tällaista toimintaa on: osallistujaluetteloiden ylläpito, kutsu seurakunnan toimintaan, hautaustoimen asioiden hoito sekä seurakunnan tai kolmannen osapuolen etujen varmistamiseksi, tällaisia etuja ovat mm. saatavien perintä, maksuliikenteen hoitaminen tai lakisääteisten velvoitteiden hoitaminen.

Henkilöiden suostumus kirjataan ilmoittautumisen yhteydessä tai sopimuksenteon vaiheessa. Henkilötietoja säilytetään käyttötarpeen vaatiman ajan. Säilytysaikaan vaikuttaa lainsäädäntö. Asianmukaisen ja läpinäkyvän henkilötietojen käsittelyn vuoksi rekisteröidylle ihmiselle ilmoitetaan henkilötietojen säilytysaika tai säilytysajan määrittelykriteerit sopimuksen teon tai suostumuksen antamisen yhteydessä.

Ilmoittautumisella tarkoitetaan esimerkiksi kerhoon, leirille tai vapaaehtoiseksi ilmoittautumista tai seurakunnallisen toimituksen sopimisesta. Sopimuksen teolla tarkoitetaan esimerkiksi hautapaikan lunastamista, tilan vuokraamista tms.
Rekisteröidyllä henkilöllä on oikeus päästä omiin henkilötietoihin ja saada oikaisu virheellisiin tietoihin. Rekisteröity voi rajoittaa henkilötietojen käsittelyä lainsäädännön mukaisin periaattein.

Pornaisten seurakunta ei käytä henkilötietoja automaattiseen päätöksentekoon eikä seurakunta käytä henkilötietojen profilointia päätöksenteon tukena.
Rekisteröidyllä on oikeus peruuttaa suostumus henkilötietojen käsittelyyn milloin tahansa, ellei kyseessä ole seurakunnan tai kolmannen osapuolen etujen varmistaminen.
Rekisteröidyllä on oikeus tehdä valitus valvontaviranomaiselle.
Valvontaviranomaisen yhteystiedot ovat:

Tietosuojavaltuutetun toimisto
Käyntiosoite: Ratapihantie 9, 6. krs, 00520 Helsinki
Postiosoite: PL 800, 00521 Helsinki
Vaihde: 029 56 66700
Faksi: 029 56 66735
Sähköposti: tietosuoja(at)om.fi

4. Tietosuojaselosteet

Kesken

5. Henkilötietojen käsittelyohjeet

Kesken. Kuvataan rekisterikohtaisesti.

6. Prosessikaaviot rekisteröidyn oikeuksista

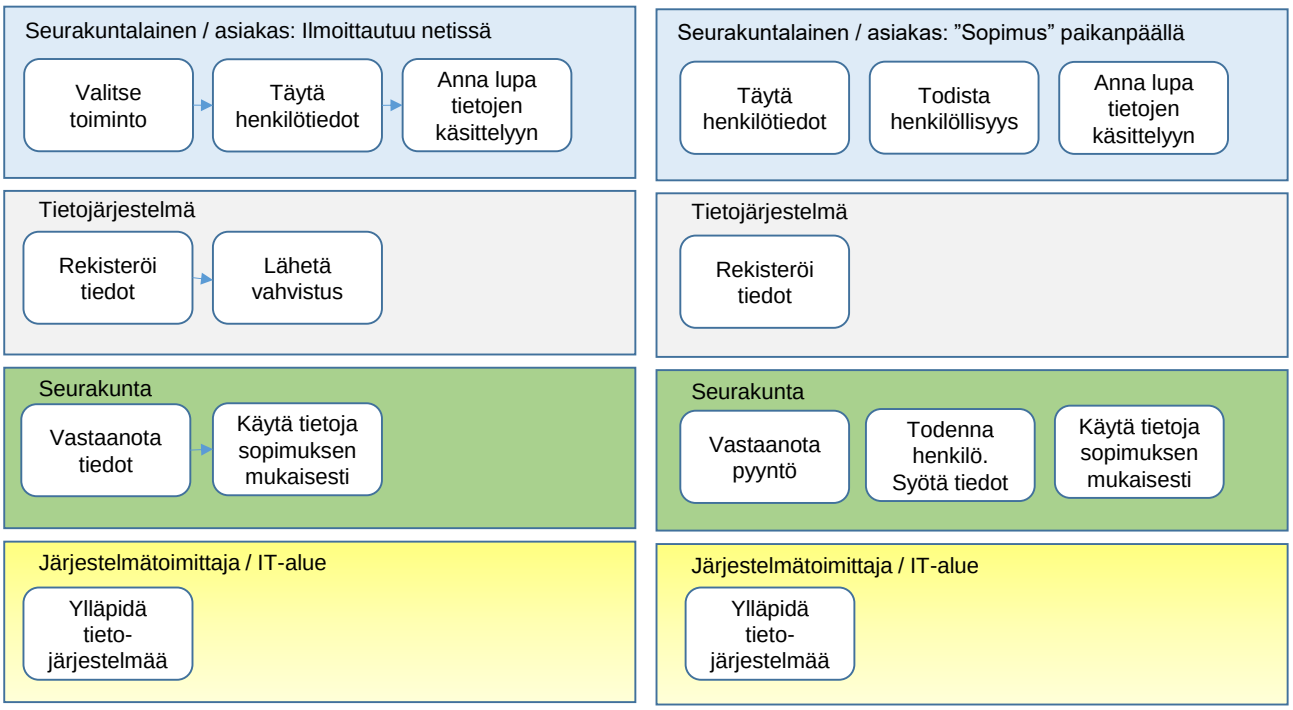
Tietosuoja-asetuksen mukaan rekisteröidyllä on oikeus virheettömiin henkilötietoihin, oikeus oikaista ja muuttaa virheelliset tiedot, oikeus vaatia tulla unohdetuksi (henkilötietojen poisto), oikeus saada tietää henkilötietojen käyttö, oikeus tietää käytetäänkö hänen henkilötietojaan profiloinnin tai automaattisen päätöksenteon tukena sekä oikeus tietää käsitelläänkö hänen henkilötietojaan vai ei.
Pornaisten seurakunnassa ei käytetä henkilötietojen profilointia eikä automaattista päätöksentekoa.
Seuraavissa kappaleissa kuvataan henkilötietojen käsittelyprosessit.

6.1. Henkilötietojen rekisteröinti

Henkilötiedot voidaan rekisteröidä Pornaisten seurakunnan rekistereihin seuraavin perustein:

1. Sopimus, jolla henkilö ja seurakunta sopivat palvelun tuottamisesta ja laskuttamisesta. Tällainen palvelu voi olla esimerkiksi hautaoikeuden lunastus tai jatkaminen, seurakuntasalin vuokraus tai muu hinnaston mukaisen suoritteen laskuttaminen asiakkaalta (seurakuntalainen tai muu henkilö)
2. Henkilö ilmoittautuu johonkin tilaisuuteen, retkelle, kerhoon tai muuhun ilmoittautumista vaativaan tapahtumaan.
3. Seurakunta hoitaa lakisääteistä tehtävää, esimerkiksi avioliittoon vihkiminen, kaste tai hautaan siunaaminen.

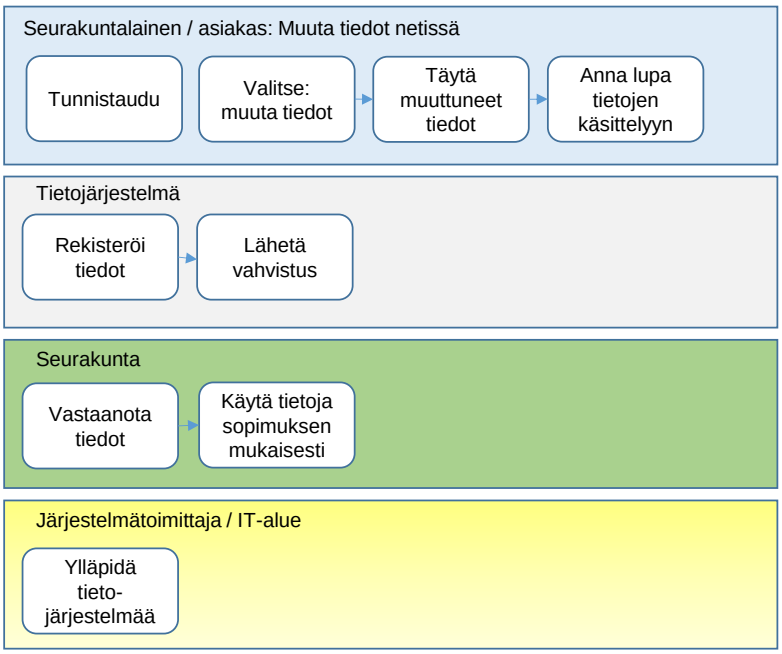
Kuvan 1 mukaan henkilö voi ilmoittautua tapahtumaan seurakunnan internet-sivujen kautta. Tällöin tietojen rekisteröinti tapahtuu automaattisesti. Toinen tapa ilmoittautua on täyttää ilmoittautumislomake ja toimittaa se seurakuntaan. Tällöin seurakunnan edustaja rekisteröi henkilötiedot henkilötietojärjestelmään.



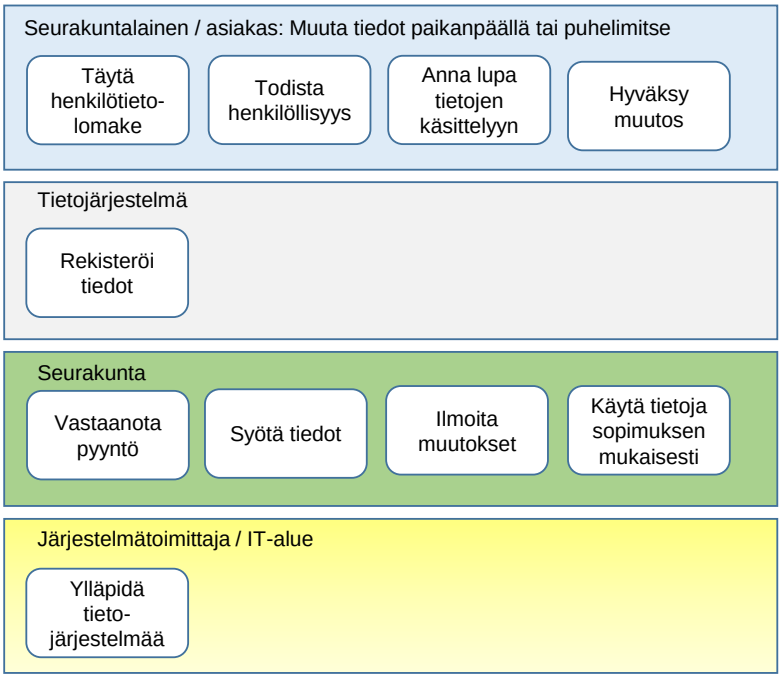
Kuva 6: Henkilötietojen rekisteröinti

6.2. Henkilötietojen muutos:

Rekisteröity voi pyytää seurakuntaa tekemään rekisteriin henkilötietomuutoksen. Myöhemmässä vaiheessa, kun tunnistautuminen on toimivaa, rekisteröity voi itse tehdä haluamansa muutoksen esimerkiksi yhteystietoihinsa. Henkilötietojen muutoksen yhteydessä todennetaan muuttajan henkilöllisyys.



Kuva 7: Henkilötietojen muutos netissä



Kuva 8: Henkilötietojen muutos paikanpäällä

7. Tietosuojatyön tiekartta; sisäinen tietosuojatyön suunnittelu ja seuranta

Kesken

8. Tietosuojavastaavan päiväkirja; mistä ja mitä neuvonut jne

Kesken

9. Tietotilinpäätös; sisäinen ja ulkoinen viestintä

Pornaisten seurakunta laatii toimintakertomuksen yhteydessä tietotilinpäätöksen Kirkkohallituksen antamien ohjeiden mukaisesti.

10. Esimerkkejä työn tuloksista

Seuraavassa on esimerkinomaisesti poiminnat Pornaisten seurakunnan dokumentaatiosta.

10.1. Osoitusvelvollisuuden toteennäyttäminen

Seuraamme osoitusvelvollisuuden täyttymistä Excel-lomakkeella. Värikoodit näyttävät tilanteen yhdellä silmäyksellä. Vihreä kertoo tilanteen olevan hallinnassa, keltainen kehottaa tarkkailemaan tilannetta ja punainen laittaa selvittämään vaihtoehtoisia ratkaisumalleja.

Taulukko 1: Tietosuoja-asetuksen tehtävien seuranta

Toimenpide / tehtävä	Selvitys	46	47	48	49	50	51	52	1	2	3	4	20	21
Tietoisku työntekijäkokouksessa														
Velvoite katsoa arjentietosuoja.fi koulutus														
Velvoite tehdä arjentietosuoja.fi testi														
Henkilö Aa, todistus		x												
Henkilö Beee, todistus		x												
Henkilö Ceee														
Henkilö Deee														
Henkilö Ähvä														
Henkilörekistereiden kartoitus														
Status hautaustoimi	Odottaa VM:n vastausta	x												
Luottamushenkilörekisteri		x												
Rippikoulurekisteri														
Kerholaistenrekisteri														
Diakonian asiakasrekisteri														
Taloushallinto - Kipa														
Henkilöstöhallinto - Kipa														
Vapaaehtoisten rekisteri														
Sopimusten kartoitus														
Nykytilan analysointi														
Riskianalyysi														
Ohjaavan dokumentaation laadinta														
Tavoitetilan määrittely														
Toimenpiteiden määrittely														
Muutosten toteuttaminen														
Toimenpiteiden esittely kirkkoneuvostolle														

	Aikataulu / suunnitelma
x	Valmis
	Ongelmia

10.2. Status hautaustoimen rekisterin kartoitus

Jokainen henkilörekisteri kartoitetaan ja analysoidaan erikseen. Kartoitusvaiheessa tutkitaan tietojen tallennustapaa ja tallennuspaikkaa. Kirjataan reksiterin vastuuhenkilö sekä pääkäyttäjät (roolit) sekä käyttöoikeuksien myöntäminen. Selvitetään miten rekisteri on suojattu sekä sopimuskumppanit. Kartoitukseen kuuluu pohtia myös rekisterin sisältämät henkilötietoluokat, henkilötiedot, käsittelyperusteet, tietojen säilytysaika ja tietovirrat. Selvitettäviin asioihin kuuluu myös rekisterin säilytyksen maantieteellinen sijainti sekä pohdinta keillä muilla toimijoilla on mahdollisuus päästä rekisterin tietoihin. Lisäksi on syytä kirjata muut eteen tulleet huomiot.

Taulukko 2: Status hautaustoimen rekisterin kartoitus

Henkilörekisterin nimi / käyttötarkoitus	**Status hautaustoimi**
Tietojen tallennustapa /-paikka	Status ohjelmisto
Tietojen tallennuspaikka	Kirkkohallituksen palvelukeskus
Rekisterin vastuuhenkilö	Toimistonhoitaja
Pääkäyttäjä	Toimistonhoitaja
Käyttöoikeudet	Toimistonhoitaja, talouspäällikkö, hautausmaanhoitaja
Suojaus	Verkon käyttäjätunnus ja salasana Sovelluksen käyttäjätunnus ja salasana
Sopimuskumppanit	Kirkkohallitus, CGI Suomi Oy
Henkilötietoluokat	Arkaluonteiset
Henkilötiedot	Nimi, yhteystiedot, vakaus,
Käsittelyperuste	Hautaustoimen asiakkuus, sopimus omaisen kanssa
Säilytysaika	
Tietovirrat	Paperituloste, siirto Exceliin
Maantieteellinen sijainti	
Muilla mahdollisesti rekisteriin pääsy	Kirkkohallituksen käyttötuki CGI:n sovelluskehitys
Huomioita	Salasana lukkiutuu x virheellisen salasanan jälkeen

10.3. Status hautaustoimen rekisterin analyysi:

Analyysissä tutkitaan henkilötietojen käsittelyperuste, joka voi olla yksiselitteinen suostumus, sopimus, seurakuntalaisen elintärkeä etu, seurakunnan etu, kolmannen osapuolen etu tai ei mikään edellä mainituista. Seuraavaksi analysoidaan käsittelyperusteen lainmukaisuus, joka voi olla: lakisääteinen velvollisuus, yleisen tehtävän hoitaminen, julkisenvallan käyttöä, käsittelyperuste voi löytyä asetuksesta tai ei mikään edellä mainituista.

Kolmanneksi analysoidaan käsitelläänkö rekisterissä erityisiä henkilöryhmiä, joita ovat: uskonnollinen vakaus, terveystieto, seksuaalisuuteen liittyvä tieto, ammattiliiton jäsenyys. Neljänneksi analysoidaan kerättävien henkilötietojen kohtuullisuus käyttötarkoitusta varten. Arviointikriteerinä ovat: kerätään vain tarvittava tieto, tietoa kerätään historiankirjoitusta varten tai tietoa kerätään varmuuden vuoksi. Viidenneksi analysoidaan

kerättyjen henkilötietojen oikeellisuuden taso. Kriteereinä ovat: lainmukaisuus, kohtuullisuus, läpinäkyvyys, tarkoituksenmukaisuus, minimointi, täsmällisyys, säilytysajan rajaus, eheys ja luottamuksellisuus .

Taulukko 3: Status-hautaustoimen rekisterin analyysi

Nykytilan analysointi - vertaa nykytilaa EU:n tietosuoja-asetuksen vaatimuksiin			
Arvion kohde	**Kriteerit**	**Valitse arvo**	**Lisäselite**
Käsittelyperuste on asetuksen mukainen	1 Yksiselitteinen suostumus 2 Sopimus 3 Seurakuntalaisen elintärkeä etu 4 Seurakunnan etu 5 Kolmannen osapuolen etu, kenen 0 Ei mikään edellä mainituista	1	Asettuessaan ehdolle henkilö on antanut suostumuksen tietojen käsittelylle
Käsittelyperuste on lain mukainen	1 Lakisääteinen velvollisuus 2 Yleisen tehtävän hoitaminen 3 Julkisen vallan käyttö 4 Käsittelyperuste asetuksesta 0 Ei mikään edellä mainituista	1	
Käsitelläänkö erityisiä henkilötietoryhmiä Kirjaa käsittelyn perustelut lisäselite kenttään	1 Uskonnollinen vakaumus 2 Terveystieto 3 Seksuaalisuuteen liittyvä tieto 4 Ammattiliiton jäsenyys 9 Ei sisällä arkaluontoista tietoa	**1**	Luottamushenkilön tulee olla ev.lut kirkon jäsen. Vakaumus ilmaistaan asettumalla ehdolle.
Henkilötietojen kohtuullisuus ja käyttötarkoituksen mukaisuus	1 Kerätään välttämätön tarvittava tieto 2 Tietoa kerätään historian kirjoitusta varten 3 Tietoa kerätään varmuuden vuoksi, voi sitä tarvita	**1**	Yhteystiedot ja palkkioiden maksatustiedot
Henkilötietojen oikeellisuus Kuvaa lisäselite kentässä miten tietoja ylläpidetään	1 Tiedot ovat ajantasalla 2 Tiedot ovat ajantasalla ja niitä päivitetään säännöllisesti 3 Tiedoissa on puutteita	2	Henkilöille lähetetään säännöllisesi postia, puuttelliset yhteystiedot estävät kokousmateriaalin saamisen
Tietojen säilytysaika Kirjaa peruste säilytysajalle	1 Tarpeen mukainen säilytysaika 2 Tietoa säilytetään varmuuden vuoksi 3 Ei tietoa säilytysajasta	1	Palkkiotiedot säilytetään palkanlaskennan edellyttämän ajan
Tietoturvan ja tietosuojan taso	1 Turvallisuudesta huolehdittu ohjeiden mukaisesti 3 Epäselvyyttä turvallisuudesta	1	

10.4. Luottamushenkilörekisterin kartoitus:

Luottamushenkilörekisterin osalta tehdään sama kartoitus, kuin tehtiin Status-hautaustoimen rekisterin kanssa. Katso kohta 10.2.

Taulukko 4: Luottamushenkilörekisterin kartoitus

Henkilörekisterin nimi / käyttötarkoitus	**Luottamushenkilörekisteri / yhteydenpito luottamushenkilöihin**
Tietojen tallennustapa /-paikka	Populus, Katriina ja Excel taulukko
Tietojen tallennuspaikka	Hallinnon kansio, Kirkkovaltuusto. Tietojärjestelmät
Rekisterin vastuuhenkilö	Talouspäällikkö
Pääkäyttäjä	Toimistonhoitaja
Käyttöoikeudet	talouspäällikkö, toimistonhoitaja, kirkkoherra
Suojaus	Verkon käyttäjätunnus, hakemiston oikeudet, sovellusten käyttöoikeudet
Sopimuskumppanit	KustensIT – käyttötuki, M&V Software, Kirkkohallitus
Henkilötietoluokat	Salassapidettävä
Henkilötiedot	Nimi, yhteystiedot, hetu
Käsittelyperuste	Suostumus ehdokkaaksi, valinta luottamushenkilöksi
Säilytysaika	Palkanlaskenta 50 vuotta
Tietovirrat	Katrian -> Excel, Populus
Maantieteellinen sijainti	Suomi
Muilla mahdollisesti rekisteriin pääsy	KustensIT, M&V Software, Kirkkohallitus

10.5. Luottamushenkilörekisterin analyysi:

Luottamushenkilörekisteri analysoidaan samalla tavalla kuin Status-hautaustoimi, katso kohta 10.3.

Taulukko 5: Luottamushenkilörekisterin analyysi

Nykytilan analysointi - vertaa nykytilaa EU:n tietosuoja-asetuksen vaatimuksiin			
Arvion kohde	**Kriteerit**	**Valitse arvo**	**Lisäselite**
Käsittelyperuste on asetuksen m	1 Yksiselitteinen suostumus 2 Sopimus 3 Seurakuntalaisen elintärkeä etu 4 Seurakunnan etu 5 Kolmannen osapuolen etu, kenen 0 Ei mikään edellä mainituista	1	Asettuessaan ehdolle henkilö on antanut suostumuksen tietojen käsittelylle
Käsittelyperuste on lain mukaine	1 Lakisääteinen velvollisuus 2 Yleisen tehtävän hoitaminen 3 Julkisen vallan käyttö 4 Käsittelyperuste asetuksesta 0 Ei mikään edellä mainituista	1	
Käsitelläänkö erityisiä henkilötietoryhmiä Kirjaa käsittelyn perustelut lisäselite kenttään	1 Uskonnollinen vakaumus 2 Terveystieto 3 Seksuaalisuuteen liittyvä tieto 4 Ammattiliiton jäsenyys 9 Ei sisällä arkaluontoista tietoa	**1**	Luottamushenkilön tulee olla ev.lut kirkon jäsen. Vakaumus ilmaistaan asettumalla ehdolle.
Henkilötietojen kohtuullisuus ja	1 Kerätään välttämätön tarvittava tieto 2 Tietoa kerätään historian kirjoitusta varten 3 Tietoa kerätään varmuuden vuoksi, voi sitä tarvita	**1**	Yhteystiedot ja palkkioiden maksatustiedot
Henkilötietojen oikeellisuus Kuvaa lisäselite kentässä miten tietoja ylläpidetään	1 Tiedot ovat ajantasalla 2 Tiedot ovat ajantasalla ja niitä päivitetään säännöllisesti 3 Tiedoissa on puutteita	2	Henkilöille lähetetään säännöllisesi postia, puuttelliset yhteystiedot estävät kokousmateriaalin saamisen
Tietojen säilytysaika Kirjaa peruste säilytysajalle	1 Tarpeen mukainen säilytysaika 2 Tietoa säilytetään varmuuden vuoksi 3 Ei tietoa säilytysajasta	1	Palkkiotiedot säilytetään palkanlaskennan edellyttämän ajan
Tietoturvan ja tietosuojan taso	1 Turvallisuudesta huolehdittu ohjeiden mukaisesti 3 Epäselvyyttä turvallisuudesta	1	